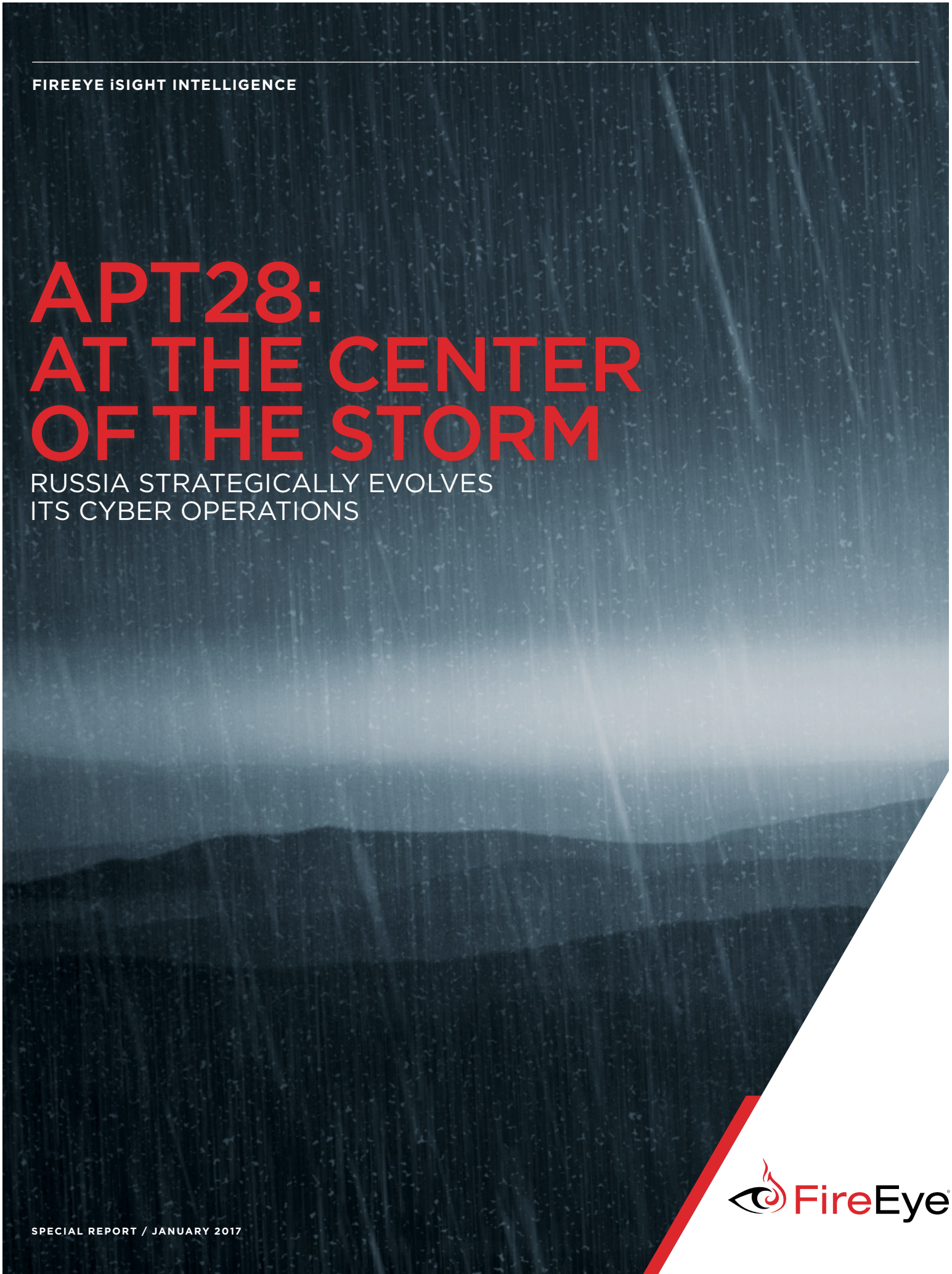


FIREEYE iSIGHT INTELLIGENCE

APT28: AT THE CENTER OF THE STORM

RUSSIA STRATEGICALLY EVOLVES ITS CYBER OPERATIONS

SPECIAL REPORT / JANUARY 2017

FireEye

CONTENTS

INTRODUCTION

The Democratic National Committee's (DNC) June 2016 announcement attributing its network breach to the Russian Government triggered an international debate over Russia's sponsorship of information operations against the U.S.

At issue is the question of proof: did the Russian Government direct the group responsible for the breaches and related data leaks? If so, is this simply a matter of accepted state espionage, or did it cross a line? Was the DNC breach part of a concerted effort by the Russian Government to interfere with the U.S. presidential election?

Unfortunately, we have failed to ask the most consequential question: how will Russia continue to employ a variety of methods, including hacks and leaks, to undermine the institutions, policies, and actors that the Russian Government perceives as constricting and condemning its forceful pursuit of its state aims?

Our visibility into the operations of APT28 - a group we believe the Russian Government sponsors - has given us insight into some of the government's targets, as well as its objectives and the activities designed to further them. We have tracked and profiled this group through multiple investigations, endpoint and network detections, and continuous monitoring. Our visibility into APT28's operations, which date to at least 2007, has allowed us to understand the group's malware, operational changes, and motivations. This intelligence has been critical to protecting and informing our clients, exposing this threat, and strengthening our confidence in attributing APT28 to the Russian Government.

OVERVIEW

On December 29, 2016, the Department of Homeland Security (DHS) and Federal Bureau of Investigation (FBI) released a Joint Analysis Report confirming FireEye's long held public assessment that the Russian Government sponsors APT28. Since at least 2007, APT28 has engaged in extensive operations in support of Russian strategic interests. The group, almost certainly compromised of a sophisticated and prolific set of developers and operators, has historically collected intelligence on defense and geopolitical issues. APT28 espionage activity has primarily targeted entities in the U.S., Europe, and the countries of the former Soviet Union, including governments and militaries, defense attaches, media entities, and dissidents and figures opposed to the current Russian Government.

Over the past two years, Russia appears to have increasingly leveraged APT28 to conduct information operations commensurate with broader strategic military doctrine. After compromising a victim organization, APT28 will steal internal data that is then leaked to further political narratives aligned with Russian interests. To date these have included the conflict in Syria, NATO-Ukraine relations, the European Union refugee and migrant crisis, the 2016 Olympics and Paralympics Russian athlete doping scandal, public accusations regarding Russian state-sponsored hacking, and the 2016 U.S. presidential election.

This report details our observations of APT28's targeting, and our investigation into a related breach. We also provide an update on shifts in the group's tool development and use, and summarize the tactics APT28 employs to compromise its victims.

APT28 TARGETING AND INTRUSION ACTIVITY

In October 2014, FireEye released APT28: A Window into Russia's Cyber Espionage Operations?, and characterized APT28's activity as aligning with the Russian Government's strategic intelligence requirements. While tracking APT28, we noted the group's interest in foreign governments and militaries, particularly those of European and Eastern European nations, as well as regional security organizations, such as the North Atlantic Treaty Organization (NATO) and the Organization for Security and Cooperation in Europe (OSCE), among others. Table 1 highlights some recent examples of this activity.

TABLE 1: APT28 TARGETING OF POLITICAL ENTITIES AND INTRUSION ACTIVITY

ENTITY	TIMEFRAME	APT28 TARGETING AND INTRUSION ACTIVITY
OSCE	NOVEMBER 2016	The OSCE confirmed that it had suffered an intrusion, which a Western intelligence service attributed to APT28.[1]
Germany's Christian Democratic Union (CDU)	APRIL - MAY 2016	Researchers at Trend Micro observed APT28 establish a fake CDU email server and launch phishing emails against CDU members in an attempt to obtain their email credentials and access their accounts.[2,3]
Pussy Riot	AUGUST 2015	APT28 targets Russian rockers and dissidents Pussy Riot via spear-phishing emails.[4]
NATO, Afghan Ministry of Foreign Affairs, Pakistani Military	JULY 2015	APT28 used two domains (nato-news.com and bbc-news.org) to host an Adobe Flash zero-day exploit to target NATO, the Afghan Ministry of Foreign Affairs, and the Pakistani military.
German Bundestag & Political Parties	JUNE 2015	Germany's Federal Office for Security in Information Technology (BSI) announced that APT28 was likely responsible for the spear phishing emails sent to members of several German political parties. The head of Germany's domestic intelligence agency, Bundesamt für Verfassungsschutz (BfV), also attributed the June 2015 compromise of the Bundestag's networks to APT28.[5,6]
Kyrgyzstan Ministry of Foreign Affairs	OCTOBER 2014 THROUGH SEPTEMBER 2015	FireEye iSight Intelligence identified changes made to domain name server (DNS) records that suggest that APT28 intercepted email traffic from the Kyrgyzstan Ministry of Foreign Affairs after maliciously modifying DNS records of the ministry's authoritative DNS servers.
Polish Government & Power Exchange websites	JUNE AND SEPTEMBER 2014	APT28 employed "Sedkit" in conjunction with strategic web compromises to deliver "Sofacy" malware on Polish Government websites, and the websites of Polish energy company Power Exchange.[7]

1. Gauquelin, Blaise. "La Russie soupçonnée d'être responsable d'un piratage informatique contre l'OSCE." Le Monde. 28 Dec. 2016. Web. 29 Dec. 2016.
2. Trend Micro refers to activity corresponding to FireEye's APT28 as "Pawn Storm."
3. Hacquebord Feike. "Pawn Storm Targets German Christian Democratic Union." Trend Micro. 11 May 2016. Web. 29 Dec. 2016.
4. Hacquebord Feike. "Pawn Storm's Domestic Spying Campaign Revealed; Ukraine and US Top Global Targets." TrendLabs Security Intelligence Blog, Trend Micro. 18 August 2015. Web. 29 Dec. 2016.
5. "Neuer Hackerangriff auf Bundespolitiker / BSI warnt Parteien vor Cyberangriffen." Westdeutscher Rundfunk. 20 Sept. 2016. Web. 29 Dec. 2016.
6. "Russia 'was Behind German Parliament Hack.'" The BBC. 13 May 2016. Web. 29 Dec. 2016.
7. Kharouni, Loucif. et al. "Operation Pawn Storm: Using Decoys to Evade Detection." Trend Micro. 22 Oct. 2014. Web. 3 Jan. 2017.

Since 2014, APT28 network activity has likely supported information operations designed to influence the domestic politics of foreign nations. Some of these operations have involved the disruption and defacement of websites, false flag operations using false hacktivist personas, and the theft of data that was later leaked publicly online.

Table 2 highlights incidents in which victims suffered a compromise that FireEye iSIGHT Intelligence, other authorities, or the victims themselves later attributed to the group we track as APT28. All of these operations have aimed to achieve a similar objective: securing a political outcome beneficial to Russia.

TABLE 2: APT28 NETWORK ACTIVITY HAS LIKELY SUPPORTED INFORMATION OPERATIONS

VICTIM	TIMEFRAME	APT28 NETWORK ACTIVITY	ASSOCIATED INFORMATION OPERATIONS ACTIVITY
World Anti-Doping Agency (WADA)	SEPTEMBER 2016	On September 13, WADA confirmed that APT28 had compromised its networks and accessed athlete medical data.[8]	On September 12, 2016, the "Fancy Bears' Hack Team" persona claimed to have compromised WADA and released athletes' medical records as "proof of American athletes taking doping."[9]
U.S. Democratic National Committee (DNC)	APRIL – SEPTEMBER 2016	The DNC announced it had suffered a network compromise and that a subsequent investigation found evidence of two breaches, attributed to APT28 and APT29. FireEye analyzed the malware found on DNC networks and determined that it was consistent with our previous observations of APT28 tools.[10,11]	In June 2016, shortly after the DNC's announcement, the Guccifer 2.0 persona claimed responsibility for the DNC breach and leaked documents taken from the organization's network. Guccifer 2.0 continued to leak batches of DNC documents through September.[12,13]
John Podesta	MARCH – NOVEMBER 2016	Investigators found that John Podesta, Hillary Clinton's presidential campaign chairman, was one of thousands of individuals targeted in a mass phishing scheme using shortened URLs that security researchers attributed to APT28.[14]	Throughout October and into early November, WikiLeaks published 34 batches of email correspondence stolen from John Podesta's personal email account. Correspondence of other individuals targeted in the same phishing campaign, including former Secretary of State Colin Powell and Clinton campaign staffer William Rinehart, were published on the "DC Leaks" website.[15]
U.S. Democratic Congressional Campaign Committee (DCCC)	MARCH - OCTOBER 2016	In July, the DCCC announced that it was investigating an ongoing "cybersecurity incident" that the FBI believed was linked to the compromise of the DNC. House Speaker Nancy Pelosi later confirmed that the DCCC had suffered a network compromise. Investigators indicated that the actors may have gained access to DCCC systems as early as March.[16,17,18]	In August, the Guccifer 2.0 persona contacted reporters covering U.S. House of Representative races to announce newly leaked documents from the DCCC pertaining to Democratic candidates. From August to October, Guccifer 2.0 posted several additional installments of what appear to be internal DCCC documents on "his" WordPress site.[19,20]
TV5Monde	FEBRUARY 2015, APRIL 2015	In February, FireEye identified CORESHELL traffic beaconing from TV5Monde's network, confirming that APT28 had compromised TV5Monde's network.	In April 2015, alleged pro-ISIS hacktivist group CyberCaliphate defaced TV5Monde's websites and social media profiles and forced the company's 11 broadcast channels offline. FireEye identified overlaps between the domain registration details of CyberCaliphate's website and APT28 infrastructure.[21]
Ukrainian Central Election Commission (CEC)	MAY 2014	Ukrainian officials revealed that the investigation into the compromise of the CEC's internal network identified malware traced to APT28.[22]	During the May 2014 Ukrainian presidential election, purported pro-Russian hacktivists CyberBerkut conducted a series of malicious activities against the CEC including a system compromise, data destruction, a data leak, a distributed denial-of-service (DDoS) attack, and an attempted defacement of the CEC website with fake election results.[23]

8. "WADA Confirms Attack by Russian Cyber Espionage Group." World Anti-Doping Agency. 13 Sept. 2016. Web. 29 Dec. 2016.
9. Fancy Bears' HT (fancybears). "@AnonPress Greetings. We hacked #WADA. We have Proof of American Athletes taking doping. Fancybear.net." 12 Sept. 2016, 4:12 PM. Tweet.
10. CrowdStrike refers to activity corresponding to FireEye's APT28 and APT29 as "Fancy Bear" and "Cozy Bear," respectively.
11. "Nakashima, Ellen. "Cyber Researchers Confirm Russian Government Hack of Democratic National Committee." The Washington Post. 20 June 2016. Web. 29 Dec. 2016.
12. "Rid, Thomas. "All Signs Point to Russia Being Behind the DNC Hack." Motherboard, Vice. 25 July 2016. Web. 29 Dec. 2016.
13. "Bennett, Cory. "Guccifer 2.0 Drops More DNC Docs." Politico. 13 Sept. 2016. Web. 2 Jan. 2017. <>
14. Perlroth, Nicole. Shear, Michael D. "Private Security Group Says Russia was Behind John Podesta's Email Hack." The New York Times. 21 Oct. 2016. Web. 2 Jan. 2017.
15. "Franceschi-Bicchierai, Lorenzo. "How Hackers Broke Into John Podesta and Colin Powell's Gmail Accounts." 20 Oct. 2016. Web. 2 Jan. 2017.
16. "Nakashima, Ellen. "FBI Probes Suspected Breach of Another Democratic Organization by Russian Hackers." The Washington Post. 29 July 2016. Web. 29 Dec. 2016.
17. "Pelosi, Nancy. "DCCC Cyber Breach." 13 August 2016. Email. U.S. House of Representatives. Washington, DC. Politico. Web. 29 Dec. 2016.
18. "Lipton, Eric. Shane, Scott. "Democratic House Candidates Were Also Targets of Russian Hacking." The New York Times. 13 Dec. 2016. Web. 29 Dec. 2016.
19. Ibid.

FROM OLYMPIC SLIGHT TO DATA LEAK:
Investigating APT28 at the World Anti-Doping Agency

As news of the DNC breach spread, APT28 was preparing for another set of operations: countering the condemnation that Russia was facing after doping allegations and a threatened blanket ban of the Russian team from the upcoming Rio Games. Russia, like many nations, has long viewed success in the Olympic Games as a source of national prestige and soft power on the world stage. The doping allegations and prospective ban from the Games further ostracized Russia, and likely provided motivation to actively counter the allegations by attempting to discredit anti-doping agencies and policies. Our investigation of APT28's compromise of WADA's network, and our observations of the surrounding events reveal how Russia sought to counteract a damaging narrative and delegitimize the institutions leveling criticism.

ALLEGATIONS OF RUSSIAN ATHLETES' WIDESPREAD DOPING

NOV (2015)

WADA declares the Russian Anti-Doping Agency (RUSADA) non-compliant.[24]

JULY 18

WADA-commissioned report documents evidence of Russian athletes' widespread doping.[25]

AUG 4

Russian athletes were barred from competing in the Olympic Games.[26]

APT28 COMPROMISES WADA

EARLY AUG

APT28 sends spear phishing emails to WADA employees.[27]

AUG 10

APT28 uses a legitimate user account belonging to a Russian athlete to log into WADA's Anti-Doping Administration and Management System (ADAMS) database.[28]

AUG 25-SEP 12

APT28 gains access to an International Olympic Committee account created specifically for the 2016 Olympic Games, and views and downloads athlete data.[29]

FALSE HACKTIVIST PERSONAS CLAIM TO TARGET WADA, LEAK ATHLETE DATA

AUG 9

The actor @anpoland, purporting to represent "Anonymous Poland," claims to have defaced the WADA website.[30]

AUG 11

On August 11 @anpoland threatens to conduct a DDoS attack against and leak data from WADA, but fails to follow through on the threats.[31,32]

SEP 12

"Fancy Bears' Hack Team", a previously unknown group purporting to be affiliated with Anonymous, claims via Twitter to have compromised WADA, and directs readers to a website hosting stolen documents.[33]

In tweets to international journalists and Twitter accounts that disseminate hacktivist and information security news, "Fancy Bears' Hack Team" claims to have "proof of American athletes taking doping."[34]

SEP 13

WADA releases a statement confirming the breach and attributes the compromise and theft of athlete medical data to APT28.[35]

SEP 15-30

"Fancy Bears' Hack Team" releases five additional batches of medical files for high-profile athletes from multiple nations, including the U.S., which had applied for and received Therapeutic Use Exemptions (TUEs) for medications otherwise banned from competition.[36]

Claiming to support "fair play and clean sport," Fancy Bears' Hack team calls TUEs "licenses for doping."[37]

Based on this timeline of leak and threatened leak activity, as well as strikingly similar characteristics and distribution methods shared between @anpoland and "Fancy Bears' Hack Team," the same operators are highly likely behind the two personas. WADA officials, citing evidence provided by law enforcement, stated that the threat activity originated in Russia, possibly in retaliation for WADA's exposure of Russia's expansive, state-run doping.[38] The statement prompted denials from the Russian Government, with Russian sports minister Vitaly Mutko asking, "How can you prove that the hackers are Russian? You blame Russia for everything, it is very in fashion now."[39]

20. Gallagher, Sean. "Guccifer 2.0 Posts DCCC Docs, Says They're From Clinton Foundation." Ars Technica. 4 Oct. 2016. Web. 3 Jan. 2017.
21. "Russian Hackers Suspected in French TV Cyberattack." Deutsche Welle. 6 Oct. 2015. Web. 29 Dec. 2016.
22. Joselow, Gabe. "Election Cyberattacks: Pro-Russia Hackers Have Been Accused in Past." NBC News. 3 Nov. 2016. Web. 29 Dec. 2016.
23. Clayton, Mark. "Ukraine Election Narrowly Avoided 'Wanton Destruction' From Hackers (+Video)." The Christian Science Monitor. 17 June 2014. Web. 2 Jan. 2017.
24. "Foundation Board Media Release: WADA Strengthens Anti-Doping Worldwide." World Anti-Doping Agency. 18 November 2015.
25. "Russia State-Sponsored Doping Across Majority of Olympic Sports, Claims Report." The BBC. 18 July 2016. Web. 29 Dec. 2016.
26. Macguire, Eoghan. Almasy, Steve. "271 Russian Athletes Cleared for Rio Games." CNN. 5 August 2016. Web. 29 Dec. 2016.
27. "Cyber Security Update: WADA's Incident Response." World Anti-Doping Agency. 5 Oct. 2016. Web. 3 Jan. 2017.
28. "WADA Confirms Attack by Russian Cyber Espionage Group." World Anti-Doping Agency. 13 Sept. 2016.
29. "WADA Confirms Another Batch of Athlete Data Leaked by Russian Cyber Hackers 'Fancy Bear.'" World Anti-Doping Agency. 14 Sept. 2016. Web. 29 Dec. 2016. <>
30. [OP PL]. "www.tas-cas.org." Online video clip. YouTube. YouTube, 9 Aug. 2016. Web. 3 Jan. 2017.
31. Anonymous Poland (@anpoland). "@Cryptomeorg @ben_rumsby @PogoWasRight @Jason_A_Murdock @Cyber_War_News @kevincollier Tomorrow will ddos WADA and publish some secret dosc." 11 Aug 2016 10:10 AM. Tweet.
32. Anonymous Poland (@anpoland). "@JoeUchill within a few days will be new attack on the WADA/Olimpic." 5 Sept. 2016 5:19 AM. Tweet.
33. Fancy Bears' HT (fancybears). "@AnonPress Greetings. We hacked #WADA. We have Proof of American Athletes taking doping. Fancybear.net."
34. Ibid.
35. "WADA Confirms Attack by Russian Cyber Espionage Group."World Anti-Doping Agency.13 Sept. 2016.
36. Russian Hackers Leak Simone Biles and Serena Williams Files." The BBC. 13 Sept. 2016. Web. 29 Dec. 2016.
37. Rumsby, Ben. "US Superstars Serena and Venus Williams and Simone Biles Given Drugs Exemption, Russian Hackers Reveal." The Telegraph. 14 Sept. 2016. Web. 29 Dec. 2016.
38. Luhn, Alec."Fancy Bears Origins Unclear But Russia Seizes Chance to Put Boot into Wada." 15 Sept. 2016. Web. 29 Dec. 2016.
39. Gibson, Owen. "Russian Sports Minister Vitaly Mutko Denies Link to Wada Hackers." The Guardian. 14 Sept. 2016. Web. 29 Dec. 2016.

CONCLUSION

Since releasing our 2014 report, we continue to assess that APT28 is sponsored by the Russian Government. We further assess that APT28 is the group responsible for the network compromises of WADA and the DNC and other entities related to the 2016 U.S. presidential election cycle. These breaches involved the theft of internal data - mostly emails – that was later strategically leaked through multiple forums and propagated in a calculated manner almost certainly intended to advance particular Russian Government aims. In a report released on January 7 2017, the U.S. Directorate of National Intelligence described this activity as an "influence campaign."

This influence campaign - a combination of network compromises and subsequent data leaks - aligns closely with the Russian military's publicly stated intentions and capabilities. Influence operations, also frequently called "information operations," have a long history of inclusion in Russian strategic doctrine, and have been intentionally developed, deployed, and modernized with the advent of the internet. The recent activity in the U.S. is but one of many instances of Russian Government influence operations conducted in support of strategic political objectives, and it will not be the last. As the 2017 elections in Europe approach - most notably in Germany, France, and the Netherlands - we are already seeing the makings of similarly concerted efforts.

APPENDIX:
APT28's Tools, Tactics, and Operational Changes

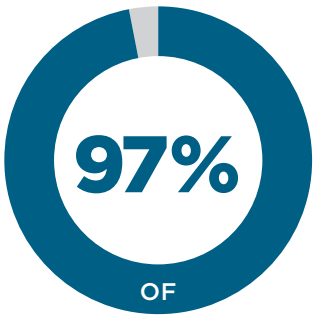
In our 2014 report, we identified APT28 as a suspected Russian government-sponsored espionage actor. We came to this conclusion in part based on forensic details left in the malware that APT28 had employed since at least 2007. We have provided an updated version of those conclusions, a layout of the tactics that they generally employ, as well as observations of apparent tactical shifts. For full details, please reference our 2014 report, APT28: A Window into Russia's Cyber Espionage Operations?

APT28 employs a suite of malware with features indicative of the group's plans for continued operations, as well as the group's access to resources and skilled developers.

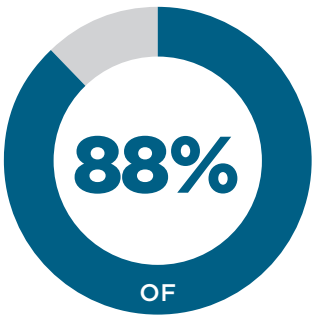
Key characteristics of APT28's toolset include:

- **A flexible, modular framework** that has allowed APT28 to consistently evolve its toolset since at least 2007.
- **Use of a formal coding environment** in which to develop tools, allowing the group to create and deploy custom modules within its backdoors.
- **Incorporation of counter-analysis capabilities** including runtime checks to identify an analysis environment, obfuscated strings unpacked at runtime, and the inclusion of unused machine instructions to slow analysis.
- **Code compiled during the normal working day in the Moscow time zone and within a Russian language build environment.**

OVER



APT28'S MALWARE SAMPLES WERE COMPILED **DURING THE WORKING WEEK**



SAMPLES COMPILED BETWEEN **8AM AND 6PM** IN THE TIMEZONE THAT INCLUDES MAJOR RUSSIAN CITIES SUCH AS MOSCOW AND ST. PETERSBURG

IN ADDITION, APT28'S DEVELOPERS **CONSISTENTLY BUILT MALWARE IN RUSSIAN LANGUAGE** SETTINGS UNTIL

2013

APT28'S MALWARE SUITE

TOOL	ROLE	AKA
CHOPSTICK	backdoor	Xagent, webhp, SPLM, (.v2 fysbis)
EVILTOSS	backdoor	Sedreco, AZZY, Xagent, ADVSTORESHELL, NETUI
GAMEFISH	backdoor	Sednit, Seduploader, JHUHUGIT, Sofacy
SOURFACE	downloader	Older version of CORESHELL, Sofacy
OLDBAIT	credential harvester	Sasfis
CORESHELL	downloader	Newer version of SOURFACE, Sofacy

APT28'S OPERATIONAL CHANGES SINCE 2014

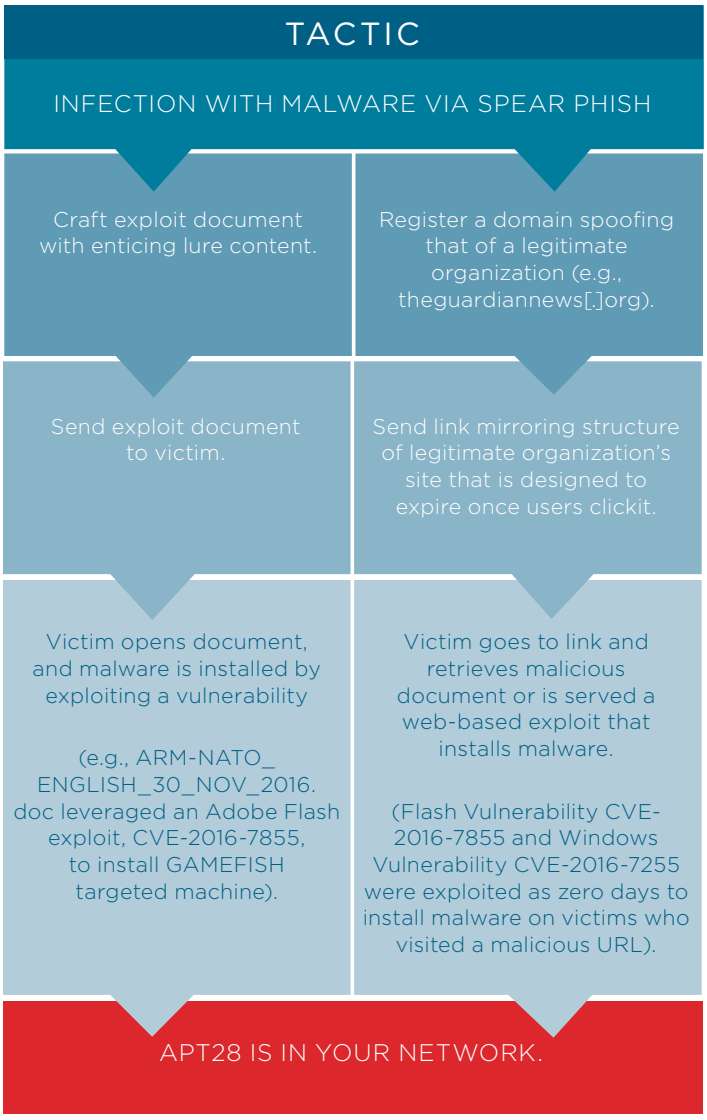
APT28 continues to evolve its toolkit and refine its tactics in what is almost certainly an effort to protect its operational effectiveness in the face of heightened public exposure and scrutiny. In addition to the continued evolution of the group's first stage tools, we have also noted APT28:

- **Leveraging zero-day vulnerabilities** in Adobe Flash Player, Java, and Windows, including CVE-2015-1701, CVE-2015-2424, CVE-2015-2590, CVE-2015-3043, CVE-2015-5119, and CVE-2015-7645.
- **Using a profiling script** to deploy zero-days and other tools more selectively, decreasing the chance that researchers and others will gain access to the group's tools.
- **Increasing reliance on public code depositories**, such as Carberp, PowerShell Empire, P.A.S. webshell, Metasploit modules, and others in a likely effort to accelerate their development cycle and provide plausible deniability.
- **Obtaining credentials through fabricated Google App authorization and Oauth access** requests that allow the group to bypass two-factor authentication and other security measures.
- **Moving laterally through a network relying only on legitimate tools** that already exist within the victims' systems, at times forgoing their traditional toolset for the duration of the compromise.

These changes are not only indicative of APT28's skills, resourcefulness, and desire to maintain operational effectiveness, but also highlight the longevity of the group's mission and its intent to continue its activities for the foreseeable future.

APT28 TACTICS

We have observed APT28 rely on four key tactics when attempting to compromise intended targets. These include sending spear-phishing emails that either deliver exploit documents that deploy malware onto a user's systems, or contain a malicious URL designed to harvest the recipients' email credentials and provide access to the their accounts. APT28 has also compromised and placed malware on legitimate websites intending to infect site visitors, and has gained access to organizations by compromising their web-facing servers



TACTIC

INFECTION WITH MALWARE VIA STRATEGIC WEB COMPROMISE (SWC)

Compromise a legitimate site and set up malicious iFrame.

Users of the site are redirected using malicious iFrame and profiled

(e.g, this technique was used to compromise and infect visitors to numerous Polish Government websites in 2014).

Exploit is served to users matching the target profile and malware is installed on their system.

APT28 IS IN YOUR NETWORK.

TACTIC

ACCESS THROUGH INTERNET-FACING SERVERS

Network reconnaissance to find vulnerable software.

Exploitation of previously known vulnerabilities present on unpatched systems.

Leverage initial compromise to access other systems and move deeper into the victim network.

APT28 IS IN YOUR NETWORK.

To download this or other
FireEye iSIGHT Intelligence reports,
visit: **www.fireeye.com/reports.html**

FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035
408.321.6300 / 877.FIREEYE (347.3393) / info@FireEye.com

www.FireEye.com

FireEye