The Recorded Future Blog

Running for Office: Russian APT Toolkits Revealed

Analysis Summary

- Russian APTs regularly target Microsoft products with 55% of exploited vulnerabilities targeting versions of Office, Windows, and Internet Explorer products. Targeting widely adopted software provides the path of least resistance for a state-sponsored actor.
- Microsoft Office vulnerability targeting is in line with heavy use of spear phishing by Russian actors including APT28. Decoy (lure) attachments are

Posted by
RFSID

August 4, 2016 in Cyber Threat Intelligence

Search ...

SEARCH

Recent Posts

Now Available: All-Source Analysis Capability
By Glenn Wong on August 8, 2016

Running for Office: Russian APT Toolkits Revealed

often Excel files or Word documents.

- APT28, associated by many with Russian military intelligence (GRU), has 22 known exploited vulnerabilities in its toolkit. Seven of these vulnerabilities have no available public exploit.
- APT29, associated by many with the Russian Federal Security Service (FSB), utilizes five known exploited vulnerabilities with no vulnerability overlap with APT28.
- 73% of vulnerabilities targeted by Russian APTs have available public exploits posted to various corners of the web including Metasploit, Exploit Database, and GitHub.
- 46% of known Russian APT exploited vulnerabilities are also found in exploit kits used by cyber criminals.

Recorded Future analysis of Russian hacking collectives has highlighted 33 known exploited product vulnerabilities used by various groups to steal information or compromise victim computers. 27 of these are tied to APT28 and APT29, collectives known by many names and possibly associated with Russian military intelligence (GRU) and the Federal Security Service (FSB) respectively.

Recent attacks and alleged subsequent leaks of stolen information from the Democratic National Committee (DNC) have highlighted the unprecedented impact of Russian threat actors in the 2016 United States Presidential election. In June 2016, Crowdstrike identified APT28 and APT29's presence in the DNC's computer systems. APT28 gained access in April 2016, while APT29 gained access in summer 2015.

By RFSID on August 4, 2016

Get Fired up About Threat Intelligence With Recorded Future at Black Hat 2016

By Amanda McKeon on July 28, 2016

Whiteboard Workflow Series: Infrastructure Vulnerability Management

By Filip Reesalu on July 27, 2016

6 Surprising Benefits of Threat Intelligence From the Web

By Pete Hugh on July 26, 2016

These actors, as well as alleged Russian state-sponsored groups Energetic Bear and Turla, regularly exploit multiple products in the Microsoft family (Office, Internet Explorer, and Windows). This is likely due to their massive user base and — in the case of Office — association with email attachment-based attacks. 55% of known leveraged vulnerabilities belong to the Microsoft family.

Interestingly, only 46% of the known exploited vulnerabilities were seen in cyber criminal-focused exploit kits. 73% of the known exploited vulnerabilities had public exploits available on forums, blogs, paste sites, and code repositories such as Exploit Database, Metasploit, and GitHub.

This suggests some element of unique capability. For instance, APT28 utilizes seven exploited vulnerabilities for which there are no available public exploits. However, in the case of Energetic Bear, public exploits make up its entire toolkit according to Kaspersky research and the below table.

Methodology

This analysis focused on advanced persistent threats (APTs) and malware families tied to likely Russian state sponsor. Recorded Future analyzed web sources including blogs, forums, paste sites, code/malware repositories, social media, and posted PDFs of finished reports and presentations.

This approach is akin to a meta-analysis.

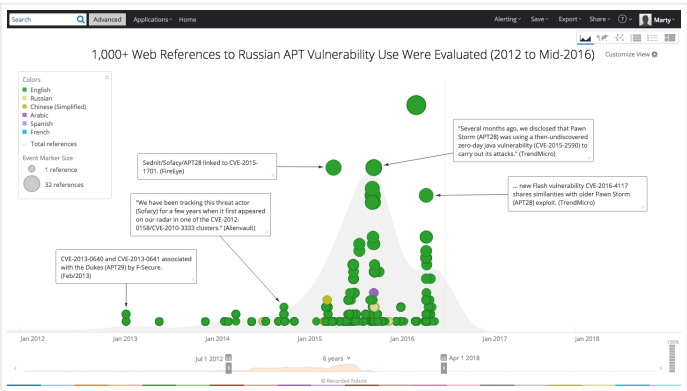
No original analysis of malware samples was conducted. The goal of this analysis was to highlight

broad trends and tactics employed by Russian threat actors.

Attack attribution and identifying threat actor plans and intentions are the hardest problems in intelligence analysis. Recorded Future makes no specific claims to recent and high-profile attacks against United States presidential candidates or campaigns.

Scope

Using Recorded Future, we analyzed information published to the web linking Russian APTs to exploited vulnerabilities from January 1, 2012 to July 31, 2016.



Subsequent analysis was conducted, applying the list of 33 known exploited vulnerabilities against Recorded Future holdings of available exploits and exploit kits frequented by cyber criminals and generally available for sale on deep and dark web (onion) forums.

As noted in previous Recorded Future APT research, analysis is complicated by the wide variety of branding and codewords applied to different facets of the problem. Some are grouped by signatures, some by actors, others by tools. Recorded Future

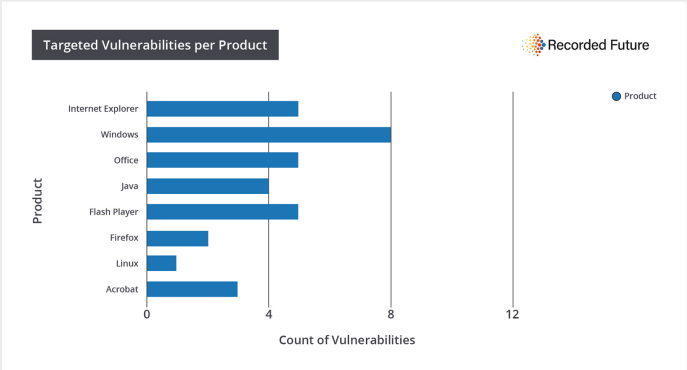
ontologies and Threat Actor Intel Cards supported this analysis which focused on the following four Russian-linked APTs/malware families:

- APT28 AKA Fancy Bear, Operation Pawn Storm, Strontium, Sednit, Sofacy, Tsar Team. Possibly associated with the Russian military's Main Intelligence Department or GRU (Главное Разведывательное Управление).
- APT29 AKA Cozy Bear, The Dukes, Office Monkeys. Possibly associated with Russia's primary intelligence service the Federal Security Service or FSB (Федеральная служба безопасности Российской Федерации), the successor to the KGB.
- Energetic Bear AKA Crouching Yeti, Dragonfly, Group 24, Koala Team. Associated with Havex malware.
- Turla AKA Epic Turla, Snake, Ouroboros, Carbon. Possibly associated to Agent.BTZ campaign.

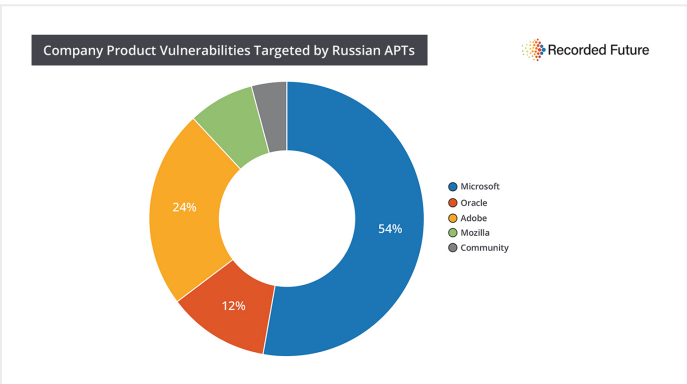
While not covered in this report, APT28, APT29, Energetic Bear, and Turla all target information consistent with Russian intelligence goals of collection on strategic adversaries, neighbors, energy targets, etc. Links to excellent research from FireEye, TrendMicro, Kaspersky, Microsoft, Crowdstrike, etc. are provided as appropriate.

Results

The following products were regularly targeted by the four Russian groups:



Organized by company:



Exploited Vulnerabilities Linked to Russian APTs

Recorded Future

	Vulnerability	Company	Product	Specific APT	Exploit Kit Presence	Exploit Available
1	CVE-2016-4117	Adobe	Flash Player	APT28	Yes	No
2	CVE-2016-0728	Community	Linux	APT28	No	Yes
3	CVE-2015-7645	Adobe	Flash Player	APT28	Yes	Yes
4	CVE-2015-5119	Adobe	Flash Player	APT28	Yes	Yes
5	CVE-2015-4902	Oracle	Java	APT28	No	No
6	CVE-2015-3043	Adobe	Flash Player	APT28	No	Yes
7	CVE-2015-2590	Oracle	Java	APT28	No	No
8	CVE-2015-2424	Microsoft	Office	APT28	No	No
9	CVE-2015-2387	Microsoft	Windows	APT28	No	No
10	CVE-2015-1701	Microsoft	Windows	APT28	No	Yes
11	CVE-2015-1641	Microsoft	Office	APT28	Yes	Yes
12	CVE-2014-6332	Microsoft	Internet Explorer	APT28	Yes	Yes
13	CVE-2014-4114	Microsoft	Windows	APT28	Yes	Yes
14	CVE-2014-4076	Microsoft	Windows	APT28	No	Yes
15	CVE-2014-3897	Microsoft	Internet Explorer	APT28	Yes	No
16	CVE-2014-1776	Microsoft	Internet Explorer	APT28	Yes	No
17	CVE-2014-1761	Microsoft	Office	APT29	Yes	Yes
18	CVE-2014-1511	Mozilla	Firefox	APT28	No	Yes
19	CVE-2014-1510	Mozilla	Firefox	APT28	No	Yes
20	CVE-2013-5065	Microsoft	Windows	Turla	No	Yes
21	CVE-2013-3897	Microsoft	Internet Explorer	APT28	Yes	Yes
22	CVE-2013-3346	Adobe	Acrobat	Turla	No	Yes
23	CVE-2013-2465	Oracle	Java	Energetic Bear	Yes	Yes
24	CVE-2013-1347	Microsoft	Internet Explorer	APT28, Energetic Bear	Yes	Yes
25	CVE-2013-0641	Adobe	Acrobat	APT29	No	No
26	CVE-2013-0640	Adobe	Acrobat	APT29	No	Yes
27	CVE-2012-1723	Oracle	Java	Turla, Energetic Bear	Yes	Yes
28	CVE-2012-0158	Microsoft	Office	APT28	Yes	Yes
29	CVE-2011-0611	Adobe	Flash Player	Energetic Bear	Yes	Yes
30	CVE-2010-4398	Microsoft	Windows	APT29	No	Yes
31	CVE-2010-3333	Microsoft	Office	APT28	No	Yes
32	CVE-2010-0232	Microsoft	Windows	APT29, Turla	No	Yes
33	CVE-2009-1123	Microsoft	Windows	Turla	No	No

Use of the Identified Vulnerabilities

Russian APTs employ tactics similar to other cyber threat actors including targeted spear-phishing, spoofed domains supporting credential phishing, social engineering, and watering-hole attacks.

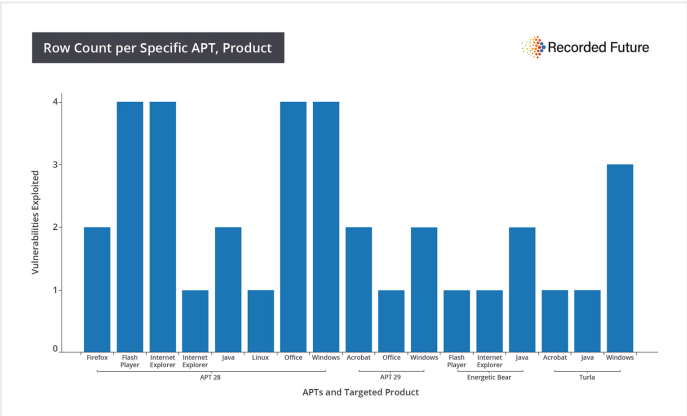
Heavy Russian APT use of Office and Adobe PDF exploits may be in line with the more targeted nature of state-sponsored attacks. Criminal campaigns such as ransomware play a numbers game, while state-sponsored attacks focus on specific organizations and information.

Previous Recorded Future analysis highlighted heavy use of Adobe Flash Player exploits in criminal exploit kits. Comparatively, five of the 33 identified vulnerabilities impacted Flash Player. Eight of the 33 impacted Office/Acrobat (generally email attachment exploits).

Siloed Approaches

Recorded Future analysis of exploited vulnerabilities used by APT28 and APT29 revealed no known overlapping use of vulnerabilities. This lends credence to the theory put forth by multiple experts that the two groups — possibly associated with GRU and FSB — don't coordinate or share resources and infrastructure. Interestingly, according to Crowdstrike, the two groups unwittingly stole the same set of DNC credentials.

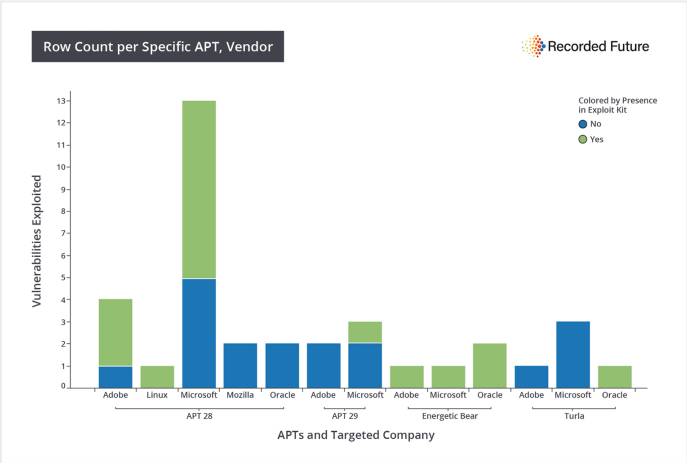
Products targeted, grouped by APT:



Overlap With Exploit Kits

46% of known Russian APT exploited vulnerabilities are also found in exploit kits used by cyber criminals. Exploit kits are available for purchase or rent on deep and dark web (onion) forums for cyber criminals seeking to deploy payloads including ransomware.

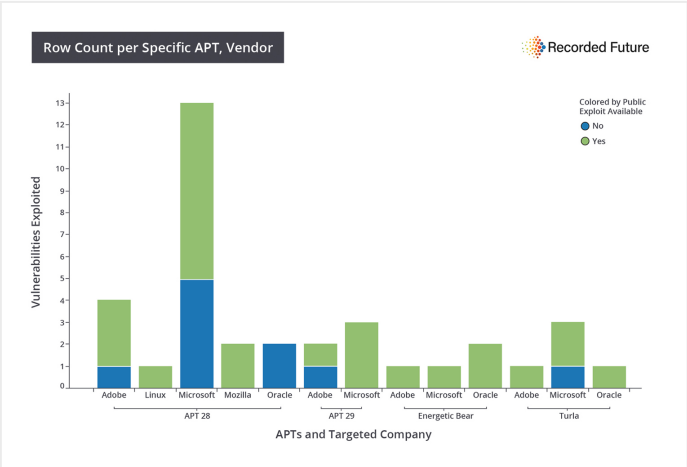
Targeted vendor, grouped by APT (colored by vulnerability present in exploit kit):



Many exploits (73%) are publicly available for these identified vulnerabilities, although the date of the publication of these exploits (versus the date of the attack) is hard to determine. Regardless, the use of common or public exploits serves a variety of purposes:

- Popular products (Windows, Office, Internet Explorer) are more likely to have well-known (and sometimes publicly available) exploits.
- Targeting popular products supports a “play the odds” approach to successful exploitation of installed software on a target computer.
- Popular product exploits help cloud efforts at attribution.

Targeted vendor, grouped by APT (colored by public availability of exploit):



Impact

With 1.5 billion people using Windows every day, and 1.2 billion people with Office products installed on their machines, the “play the odds” approach begins to explain the popularity of Microsoft products with Russian APTs.

Popular Java (used by 89% of U.S. computers) and Adobe (50 billion PDFs opened in Adobe in 2015) exploits follow this pattern. Much like with cyber criminals, the path of least resistance to a successful redirection or implant is often the best for a state-sponsored actor targeting strategic information.

Recommended Actions

We recommend you:

- Patch all vulnerabilities identified in this post.
- Conduct enterprise web and email security awareness training.
- Utilize two-factor authentication and VPNs where appropriate.
- Enforce segregation of user account privileges.

- Enable “click to play” for Adobe Flash Player in web browsers.
- Consider alternative PDF viewers.
- Monitor the web for posted email addresses (even those without paired passwords).