Krebs on Security

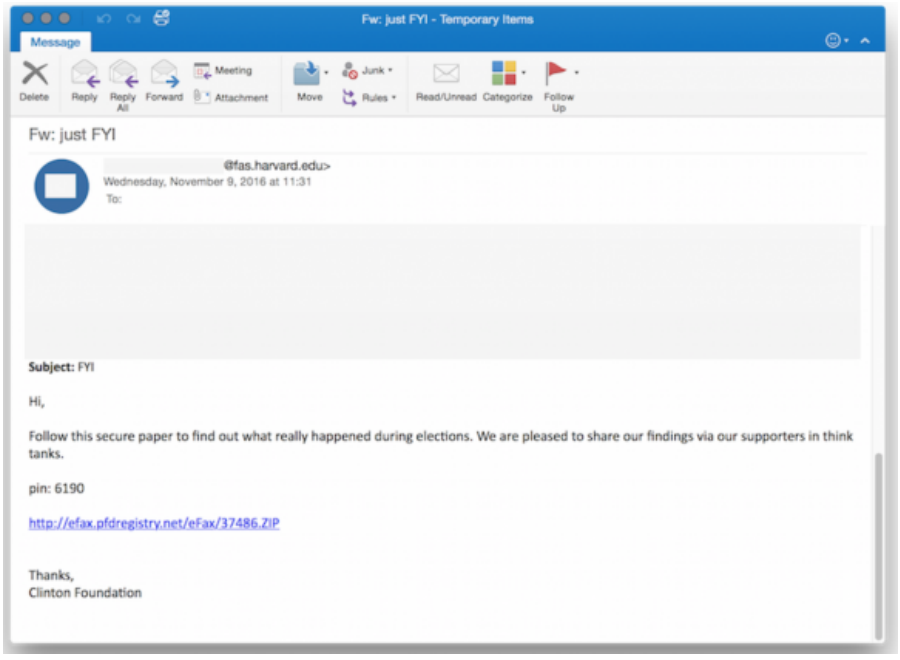
In-depth security news and investigation

- About the Author
- Blog Advertising

10
Nov 16

Russian 'Dukes' of Hackers Pounce on Trump Win

Less than six hours after Donald Trump became the presumptive president-elect of the United States, a Russian hacker gang perhaps best known for breaking into computer networks at the **Democratic National Committee** launched a volley of targeted phishing campaigns against American political think-tanks and non-government organizations (NGOs).



One of the phishing emails in the latest political espionage attack launched by The Dukes.
Source: Volexity.

That's according to a new report from Washington, D.C.-based cyber incident response firm **Volexity**. The firm's researchers say they've been closely monitoring the activities of an well-established Russian malware development gang known variously as **Cozy Bear**, **APT29**, and **The**

Dukes.

Hacking attacks launched by The Dukes were thought to be connected to intrusions at the **Democratic National Committee** (DNC), as well as cyber break-ins at multiple high-profile United States Government organizations, Volexity reports in a blog post published Thursday morning.

Last month, the Obama administration publicly acknowledged for the first time that it believed that the Russian government was responsible for stealing and disclosing emails from the DNC and a range of other institutions and prominent individuals, most recently Hillary Clinton's campaign chairman, John D. Podesta. The emails were posted on WikiLeaks and other sites.

Volexity CEO Steven Adair said The Dukes have launched at least five sorties of email-based malware phishing attacks since Trump's acceptance speech, and that the malware campaigns are ongoing.

"Two of the attacks purported to be messages forwarded on from the **Clinton Foundation** giving insight and perhaps a postmortem analysis into the elections," Adair wrote."Two of the other attacks purported to be eFax links or documents pertaining to the election's outcome being revised or rigged. The last attack claimed to be a link to a PDF download on "*Why American Elections Are Flawed*."

According to Volexity, in July 2015 the Dukes started heavily targeting think tanks and NGOs.

"This represented a fairly significant shift in the group's previous operations and one that continued in the lead up to and immediately after the 2016 United States Presidential election," Adair wrote.

Prior to the election, The Dukes were active on August 10, 2016 and on August 25, 2016, launching several waves of highly targeted spear phishing attacks against several U.S.-based think tanks and NGOs.

"These spear phishing messages were spoofed and made to appear to have been sent from real individuals at well-known think tanks in the United States and Europe," Adair wrote. "These August waves of attacks purported to be from individuals at Transparency International, the Center for a New American Security (CNAS), the International Institute for Strategic Studies (IISS), Eurasia Group, and the Council on Foreign Relations (CFR)."

Adair said the more typical attacks from The Dukes come in the form of slightly less-targeted email blasts — often to just a few dozen recipients at a time — that include booby-trapped **Microsoft Office** documents.

When launched, the tainted **Excel** or **Word** document opens an actual file with real content, but it also prompts the target to enable "macros" — a powerful functionality built into Office documents that hackers can use to automatically download and run malicious code on a Windows system.

The Dukes prefer to launch the attacks using hacked servers and email inboxes belonging to unsuspecting, trusted workers at NGOs and U.S. government systems, Adair explained. Most often, he said, the intruders will repurpose a legitimate document found in one of these hacked inboxes and inject a sophisticated backdoor "trojan horse program."

If the phishing target opens the document and has macros enabled in Microsoft Office — or allows macros to be run after the decoy document is shown — a malicious script embedded in the macro installs on the target's system a powerful foothold for the attacker.

Adair said The Dukes have a well-earned reputation for coding and constantly improving their own custom backdoor trojans, but that they're not known for using so-called "zero day" threats — previously unknown security weaknesses in software and hardware that knowledgeable attackers can use to remotely compromise a target's computer just by loading a Web page or opening a document.

"In some ways, these guys seem kind of low-budget, but their macros are well-obfuscated and will sail right through just about any [antivirus] tool, appliance or cloud service," Adair said in an interview.

The Dukes also take great care not to phish security personnel at targeted organizations. For example, if the phishing target has macros enabled in Microsoft Office or allows them to be run after the decoy document is shown, a malicious script embedded in the macro executes a busy little program that scours the target's computer for signs that it is running on an network administrator's machine.

If the malicious script detects the user is "admin" or "administrator," the infection goes no further and the malware shuts down. Likewise, it checks many other signs that it might be running in a "sandbox" environment — a test lab often used by security and malware researchers.

Adair said his although his research team doesn't have specific insight into to how successful these latest espionage attacks may have been, The Dukes are an effective information- and resource gathering machine.

"My opinion is that if this group got access to a zero-day and it's something they can embed in a document, they could devastate anyone they target," Adair said. "This is a well-funded and in some respects professional organization. What they're doing takes time and effort, and for eight plus years now they've been in continuous development of new backdoors. They're continually targeting different verticals — universities, NGOs and governments — and they learn from others, retool and modify their attacks constantly."

As *The New York Times* reported last month, "President Obama is weighing a 'proportional' response to Russia's efforts to interfere with this fall's election campaign through hacking.

Thursday morning, security vendor Kaspersky Lab warned that a massive cyberattack hit five of Russia's largest banks. Kaspersky said in a statement that the distributed denial of service attacks (DDoS) began Tuesday at 1830 IST and targeted "the websites of at least five well-known financial institutions in the top 10" in Russia.

It remains unclear who launched the bank cyberattacks, which are reportedly ongoing. Kaspersky said the attack on Russia's banking system is apparently being launched by a network of more than 24,000 hacked Internet of Things (IoT) devices, and that more than half of the hacked things

were in the United States, India, Taiwan and Israel.

Further reading on the storied hacking history of The Dukes:

F-Secure calls them CozyDuke (PDF). **FireEye**'s take (PDF). **Crowdstrike** on Cozy Bear.

Tags: APT29, Clinton Foundation, Cozy Bear, Democratic National Committee hack, Donald Trump, Microsoft macros, Office macro exploit, Steven Adair, The Dukes, Volexity

This entry was posted on Thursday, November 10th, 2016 at 12:19 pm and is filed under Other. You can follow any comments to this entry through the RSS 2.0 feed. Both comments and pings are currently closed.

78 comments

1. *anon*
November 14, 2016 at 8:47 pm

Really Brian? You are promoting this nonsense that they are state actors, without any alternative point of view being provided?

To claim this group of guys using tools that can be bought on hackforums.net for $100 are absolutely certainly being paid by the russian government is really just insane.

- *Gi*
November 16, 2016 at 2:07 pm

The phishing lure is simple, but they're not using HF tools. They're spreading Powerduke malware, which has been previously established as being tied to a Russian group targeting Georgia, Ukraine, and the DNC.

Every US intelligence agency and every major US security firm corroborates the story. No firm in any country has ever provided any evidence to the contrary, including Russia's Kaspersky firm.

CrowdStrike: https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/
Mandiant: https://www.washingtonpost.com/world/national-security/cyber-researchers-confirm-russian-government-hack-of-democratic-national-committee/2016/06/20/e7375bc0-3719-11e6-9ccd-d6005beac8b3_story.html
Fidelis: http://www.computerworld.com/article/3086314/security/russian-hackers-were-behind-dnc-breach-says-fidelis-cybersecurity.html
Dell SecureWorks: https://www.secureworks.com/research/threat-group-4127-targets-hillary-clinton-presidential-campaign
Threatconnect: https://www.threatconnect.com/blog/guccifer-2-all-roads-lead-russia/
FireEye: https://www.fireeye.com/blog/threat-research/2014/10/apt28-a-window-into-russias-cyber-espionage-operations.html
Volexity: https://www.volexity.com/blog/2016/11/09/powerduke-post-election-spear-phishing-campaigns-targeting-think-tanks-and-ngos/

Russia has the primary motive, *all* technical evidence points to Russia, a Russia state official has hinted it's true, retired and fired US intelligence officials have said it's true (and that we've done the same to other countries, so we can't necessarily complain), the private and public sectors are all in agreement, Putin obviously favors Trump politically (though Trump's election was probably just exploited strategically rather than Trump actually colluding with Putin).

It's Russia.

- *Mike*
November 17, 2016 at 1:17 pm

My vote was not given based on who Putin favors one way or the other. I see no reason why it should.

Who cares who Putin favors?

I also see no reason to use Kaspersky. The simple truth is that if people were actually interested in security instead of just making it "look" like they are, most of these problems would not ever exist.

- *Diane Wilkinson Trefethen*
November 19, 2016 at 11:48 am

@Gi – No matter how many neolibs CLAIM that the Russian government is responsible for hacking the US, claims do not equal proof. Keep in mind these ironclad sources are also responsible for claiming that Saddam Hussein had WMD (when they knew he didn't), Russia invaded Ukraine (when they knew it didn't), the attack on Benghazi was because of a movie (which it wasn't but they didn't care), and the Saran attacks were done by the Syrian government (they weren't, at least not exclusively and

conclusively). War is big business. IKE's warning has been ignored and now we are in endless, profitable, wars. When it comes to war, I trust Eisenhower a helluva lot more than people who say let you and him fight so *I* can make a freaking fortune.

- *Ed*
  November 18, 2016 at 12:32 am

  Once you folks clear the santorum-like residue of Donnycum from yor throats, you might wake up and button down *your* machines.

2. *Jim R*
   November 16, 2016 at 8:48 am

   I'm surprised that the "Russian connection" is still being peddled, which strangley enough, all Democrats pushed as a way of tying Trump to Putin. What's more likely is that Anonymous discovered the depths of corruption that Cankles McPantsuit had sunk to and decided to expose her and her cohorts. And of course all the little liberal sheep gobbled up the Russian angle…

   - *KrebsTheMan*
     November 22, 2016 at 6:38 pm

     Krebs is an expert in cyber security, try to show some respect!

     You certainly are no expert in the complexities of cyber security or international relations…

3. *Rich Graves*
   November 16, 2016 at 8:51 am

   Dear anon,

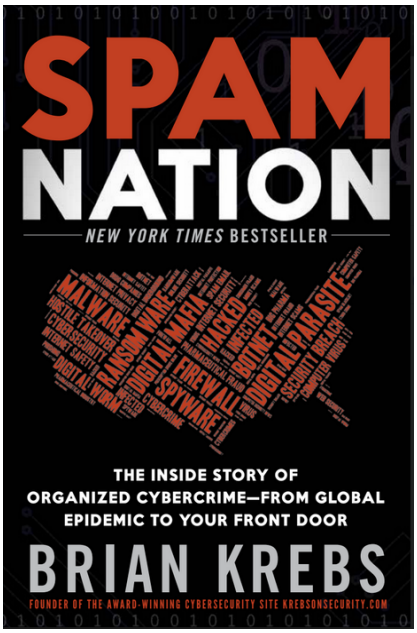
   Yes, it is important to be precise about what we do and do not know about exactly how "state-sponsored" these attackers are. As I learned from former Air Force cybersecurity officer @robtlee and other peers in graduate school, "Advanced Persistent Threat" is defined not by their advanced technical techniques, but by their persistence and motivation.

   In the case of APT1, the Chinese hackers who went after military secrets, we know that they are full time employees of the Chinese People's Liberation Army. The public Mandiant report includes their unit designation and the street address of their headquarters. While AFAIK not public, we know the names of key officers. Less is (publicly) known about the Russian APT28 "Fancy Bear" and APT 29 "Cozy Bear." I have read that one may be FSB and the other GRU, but it's also possible that they are "private" like Booz Allen Hamilton and SAIC or even (far less likely) unpaid and motivated by nationalism and the lulz. There is *no doubt* that they are Russian and intent on undermining democracy and the capacity to resist authoritarianism worldwide.

   I have seen many examples of their work. They are not going after hard miltary targets. They are going after people who advocate human rights and civil liberties.

← Older Comments

-
- **My New Book!**



A New York Times Bestseller!

- Buy at Amazon
- Donate with PayPal

Recent Posts

- How to Bury a Major Breach Notification
- February Updates from Adobe, Microsoft
- Men Who Sent Swat Team, Heroin to My Home Sentenced
- Who Ran Leakedsource.com?
- Fast Food Chain Arby’s Acknowledges Breach

Subscribe by email

Please use your primary mailbox address, not a forwarded address.

Your email:
Enter email address...

Subscribe Unsubscribe

All About Skimmers

Click image for my skimmer series.

- **The Value of a Hacked PC**

Badguy uses for your PC

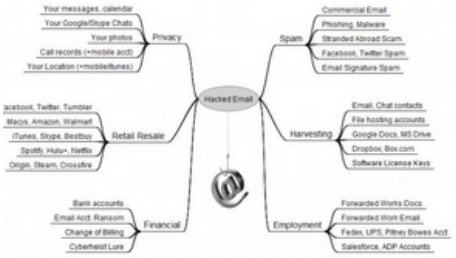
- **Tools for a Safer PC**

Tools for a Safer PC

- **The Pharma Wars**

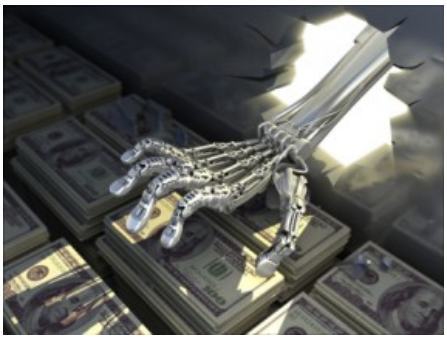
Spammers Duke it Out

- **Badguy Uses for Your Email**



Your email account may be worth far more than you imagine.

- **eBanking Best Practices**



eBanking Best Practices for Businesses

- ## Most Popular Posts

  - Online Cheating Site AshleyMadison Hacked (798)
  - Sources: Target Investigating Data Breach (620)
  - Cards Stolen in Target Breach Flood Underground Markets (445)
  - Reports: Liberty Reserve Founder Arrested, Site Shuttered (416)
  - Was the Ashley Madison Database Leaked? (376)
  - True Goodbye: 'Using TrueCrypt Is Not Secure' (363)
  - Who Hacked Ashley Madison? (360)
  - Following the Money, ePassporte Edition (353)
  - U.S. Government Seizes LibertyReserve.com (315)
  - Extortionists Target Ashley Madison Users (310)

- ## Category: Web Fraud 2.0

Innovations from the Underground

ID Protection Services Examined

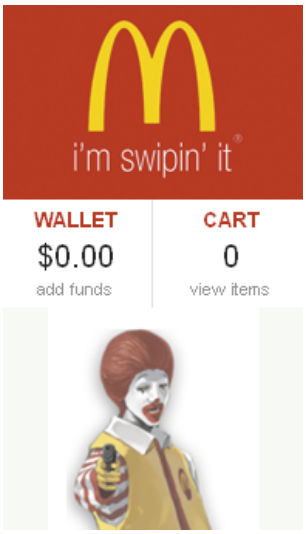
- **Is Antivirus Dead?**

The reasons for its decline

- **The Growing Tax Fraud Menace**

File 'em Before the Bad Guys Can

- **Inside a Carding Shop**



A crash course in carding.

- **Beware Social Security Fraud**

Sign up, or Be Signed Up!

- **How Was Your Card Stolen?**

Finding out is not so easy.

- **Krebs’s 3 Rules…**

...For Online Safety.
