exabeam PRODUCT ABOUT BLOG LIBRARY CONTACT GET A DEMO

Information Security Blog › Information Security › Cyber Espionage and the US Elections: What are Russian Hackers Possibly Doing and How Can They be Stopped?

INFORMATION SECURITY AUGUST 31, 2018

Cyber Espionage and the US Elections: What are Russian Hackers Possibly Doing and How Can They be Stopped?

RICHARD CASSIDY

SHARE

Russian meddling in the 2016 US elections and the Hillary Clinton campaign email breach came as a surprise to many (with investigations underway as to who knew what and who was involved). While the *New York Times* reported the Obama White House had warned the Russians about “malicious cyber activity” and later had knowledge of campaign chairman John Podesta’s Gmail hack, it decided to not publicly disclose that at the time for specific reasons.*

Two years later, alarms are again sounding about new threats from Russian bad actors targeting US elections. On August 21, Microsoft announced its Digital Crimes Unit took control of six phony web domains created to mimic US Senate and public policy sites.

With various levels of certainty, many in the security industry believe that Fancy Bear (aka, APT28, Strontium, Pawn Storm, Sofacy Group, and Sednit) are associated with the Main Intelligence Directorate (GRU), the former Soviet Union military intelligence agency. Fancy Bear has been attributed with a long list of targeted attacks against NATO-aligned states, so it’s not surprising that Microsoft took swift action to help mitigate the risk posed with the fake political websites.

Reported election-meddling activities, such as the bogus Microsoft domains, often exhibit similar techniques, tactics, and procedures (TTP) that are important for cybersecurity pros to understand. Let’s begin by reviewing TTP characteristics used in the prior US election hack.

Common TTPs of political cyber espionage

While there is no evidence that the fraudulent Microsoft domains were successfully used in

Subscribe
Email address SUBMIT

TRENDING INFORMATION SECURITY ARTICLES

1 Understanding the Role of Artificial Intelligence, Machine Learning, and Deep Learning in Cybersecurity

2 How Criminals Can Build a “Web Dossier” from Your Browser

3 GDPR and the Security Monitoring Challenge

4 Complying with NY State DFS Regulations with Exabeam

5 Extracting Actionable Information from Windows Events

prompt them to log in. Steal their credentials with the goal of gaining access to their private information, such as the DNC emails that were published by WikiLeaks.

The TTP used to deliver the malicious link can happen in a variety of ways:

- An attack relies on users clicking a malicious link, opening a malicious attachment, or falling victim to a watering hole attack. In the Podesta attack, a spear phishing email was sent to his aides, who accidentally flagged it as legitimate instead of illegitimate. It was a simple typo that had major geopolitical consequences.
- Using endpoints with vulnerabilities, victims click on websites that infect their PC, download malware, or even execute code.
- Then there are even more sophisticated approaches, such as hijacking DNS requests by way of "man-in-the-middle" attacks. These can occur when victims access websites through public wireless networks such as at hotels, coffee shops, or conference locations —often right where the hacker group is operating.
- They can also occur where a network that has been compromised is being used to farm credentials. (See Darkhotel APT group and its specific TTPs for other attack surface variations.)

Techniques for malicious email hacks are constantly changing. There are many ways to trick users into clicking a malicious link, with strategies perpetually evolving. Hackers, organized cybercrime groups, and criminal nation-state attackers rely on users not checking email sender details or the exact web address (the URL) they're visiting. The premise, "If it looks normal, it probably is" doesn't apply to cybersecurity, and it reinforces two concepts:

- You're only as strong as your weakest link (which is usually your own network users).
- Credential theft is the biggest security concern facing organizations today.

Behavioral analytics offer the best strategy for stopping cyber espionage attacks

Many organizations, equipped with legacy cybersecurity, compliance, and monitoring tools, are unable to effectively respond and thwart such attacks. Their SOC team is bombarded by an overwhelming number of alerts, which they can't begin to effectively prioritize, never mind handle. This is the bad news.

Traditional security analytics often deal with sophisticated security risks in unsophisticated ways. Outmoded toolsets rely on previous knowledge of known attacks and create specific or broad rules for detecting malicious activity. This often results in too little or too much alert data that only serve to overburden analysts; security and threat investigation teams are unable to effectively handle all the noise.

Even if organizations are able to respond to every security incident, they lack context pertaining to an actual alert. Where did it come from? Who and what is implicated? What are the artifacts or indicators of compromise (IOC) and, more importantly, what are the attack TTPs? Furthermore, there is a critical need to understand who the affected users are, and which credentials or identities are involved. What happened before, during, and after the incident? What is the degree of risk? And what is the adversary's intent?

If an attacker uses phishing to deliver malicious links, it likely comes from a new domain—and it may appear legitimate. Looking beyond the initial attack vector for a moment, consider a scenario where a user didn't notice a minute URL difference and was tricked into visiting the malicious website. Unfortunately, they revealed their credentials, so you can confidently assume the adversary is now using this to gain access to targeted resources.

Here is where many traditional security toolsets fall short. After successful login authentication, often security functions fail to monitor subsequent activity of that user. Or, if

1 The Complete Guide to CSIRT Organization: How to Build an Incident Response Team

2 Insider Threats: How to Stop the Most Common and Damaging Security Risk You Face

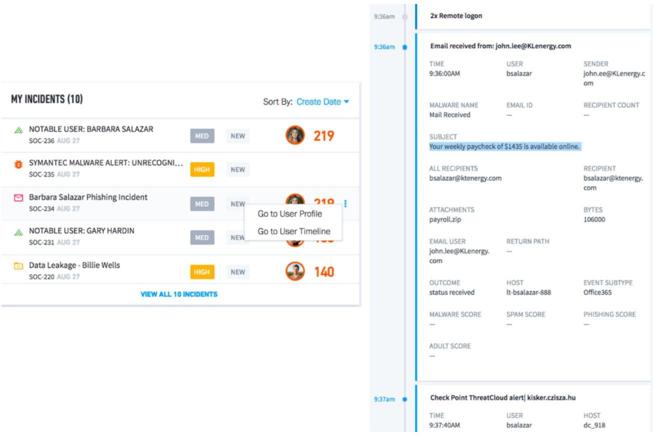
3 2018 State of the SOC Report

4 5 Best Practices for Your Incident Response Plan

5 How Criminals Can Build a "Web Dossier" from Your Browser

they do, they're only looking for specific threat events (e.g., malware delivery, identifiable IOCs, C2/backdoor activity). What resource tie all the events together?

In such cases, traditional methods might never detect a threat. The authenticated user—whoever they are—might only connect to legitimate internal or cloud-based resources, looking at sensitive data or perhaps downloading intellectual property. They might also be enumerating other network users and assets, their purpose being to gather intelligence so as to enact further malicious activities to achieve their aims.



MY INCIDENTS (10)

Sort By: Create Date

NOTABLE USER: BARBARA SALAZAR SOC-236 AUG 27	MED	NEW	219
SYMANTEC MALWARE ALERT: UNRECOGNI... SOC-235 AUG 27	HIGH	NEW	
Barbara Salazar Phishing Incident SOC-234 AUG 27	MED	NEW	219
NOTABLE USER: GARY HARDIN SOC-231 AUG 27	MED	NEW	
Data Leakage - Billie Wells SOC-220 AUG 27	HIGH	NEW	140

VIEW ALL 10 INCIDENTS

9:36am 2x Remote logon

9:36am Email received from: john.lee@KLenergy.com

TIME 9:36:00AM	USER bsalazar	SENDER john.ee@KLenergy.com
MALWARE NAME Mail Received	EMAIL ID —	RECIPIENT COUNT —
SUBJECT Your weekly paycheck of $1435 is available online.		
ALL RECIPIENTS bsalazar@ktenergy.com		RECIPIENT bsalazar@ktenergy.com
ATTACHMENTS payroll.zip		BYTES 106000
EMAIL USER john.lee@KLenergy.com	RETURN PATH —	
OUTCOME status received	HOST lt-bsalazar-888	EVENT SUBTYPE Office365
MALWARE SCORE —	SPAM SCORE —	PHISHING SCORE —
ADULT SCORE —		

9:37am Check Point ThreatCloud alert| kisker.czisza.hu

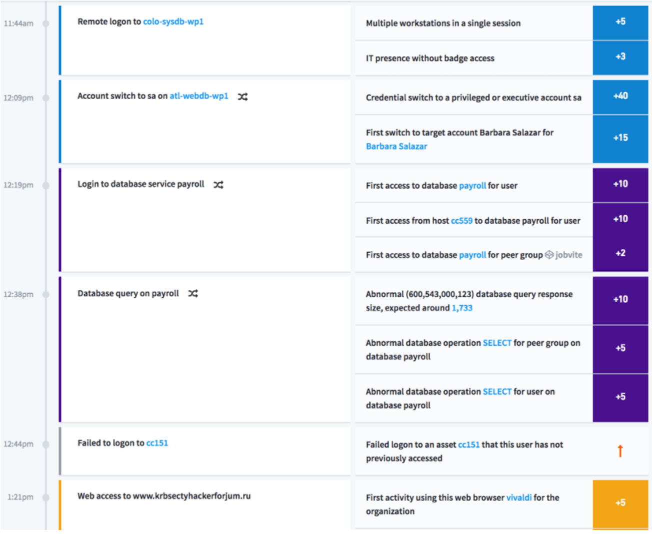
TIME 9:37:40AM	USER bsalazar	HOST dc_918

Figure 1 – A phishing incident with attached timeline showing email and associated attachments as evidence

And yet there is good news. Across all breaches there is always something that stands out as abnormal in the attack chain.

If we monitor users, credentials, assets, and user behavior for abnormalities from both an internal and external perspective, we can better thwart such attacks. By applying behavioral analytics developed through machine learning and statistical modelling, we can rapidly and effectively identify any attack vector—regardless if it has been previously seen or not.

In the previous scenario, behavioral analytics would have identified the malicious domain (from which the phishing email originated) as suspicious. This is because it's the first time that website has appeared and it isn't linked to any previous peer activity within the organization. As a result, a security incident would be created to mitigate the risk (Fig. 1).



11:44am	Remote logon to colo-sysdb-wp1	Multiple workstations in a single session	+5
		IT presence without badge access	+3
12:09pm	Account switch to sa on atl-webdb-wp1	Credential switch to a privileged or executive account sa	+40
		First switch to target account Barbara Salazar for Barbara Salazar	+15
12:19pm	Login to database service payroll	First access to database payroll for user	+10
		First access from host cc559 to database payroll for user	+10
		First access to database payroll for peer group jobvite	+2
12:38pm	Database query on payroll	Abnormal (600,543,000,123) database query response size, expected around 1,733	+10
		Abnormal database operation SELECT for peer group on database payroll	+5
		Abnormal database operation SELECT for user on database payroll	+5
12:44pm	Failed to logon to cc151	Failed logon to an asset cc151 that this user has not previously accessed	↑
1:21pm	Web access to www.krbsectyhackerforjum.ru	First activity using this web browser vivaldi for the organization	+5

Figure 2 – Timeline shows anomalous behavior (e.g., lateral movements, abnormal database access) stitched together and presented as an incident

Only through behavioral analytics can you identify abnormal and malicious activity patterns of authenticated users. For example, consider a bad actor accessing a CRM or database/data repository during an anomalous time and from a new location, or using an asset that a legitimate user wouldn't ordinarily access (Fig. 2). Behavioral analytics let you rapidly identify even the most subtle attributes of a sophisticated targeted attack and respond accordingly—before your data is unleashed and creating havoc.

——————-

*The administration feared that acknowledging Russian meddling would reveal too much about intelligence gathering and be interpreted as "taking sides" in the 2016 election, according to the former Secretary of Homeland Security.

RICHARD CASSIDY

More like this

If you'd like to see more content like this, visit the Exabeam Blog

Explore more

INFORMATION SECURITY

INFORMATION SECURITY

UEBA

Operation Aurora – 2010's Major Breach by Chinese Hackers

JANUARY 8, 2019 — TIM MATTHEWS

Exabeam's Cybersecurity History Review: Read about Operation Aurora and the series of cyberattacks in 2010 conducted by the Elderwood Group based in Beijing, China, with ties to the People's Liberation Army.

Exabeam's Top Cybersecurity Blog Posts of 2018

JANUARY 2, 2019 — MARITZA MARIE DUBEC

2018 was a memorable year for cybersecurity. Millions of people were impacted as we saw more companies hit by megabreaches—from a major hotel chain to a social media platform used by billions. Here are our top 10 blog posts that had the biggest readership and were the most noteworthy.

User Behavior Analytics (UBA/UEBA): The Key to Uncovering Insider and Unknown Security Threats

JANUARY 2, 2019 — ORION CASSETTO

Learn about UBA technology, and its extension UEBA (User Entity Behavior Analytics), how it works, and which threats it uncovers that no other tool can see.

Exabeam provides security intelligence and management solutions to help organizations of any size protect their most valuable information.

REQUEST A DEMO

PRODUCT

- Exabeam Advanced Analytics
- Exabeam Cloud Connectors
- Exabeam Data Lake
- Exabeam Entity Analytics
- Exabeam Incident Responder
- Exabeam Spectrum
- Exabeam Threat Hunter

ANALYST CORNER

PARTNERS

SUPPORT

SOLUTIONS

- Compliance
- Threat Detection
- Cloud Security
- IoT Monitoring
- SOC Automation

ABOUT

CAREERS

MEDIA KIT

LEARN

- Library
- Newsroom
- Glossary
- SIEM Cost Comparison

BLOG

- Information Security
- SIEM
- UEBA
- Security Operations Center
- DLP
- Incident Response

SIEM GUIDE

- What is SIEM?
- SIEM Architecture
- Events and Logs
- UEBA
- SIEM Use Cases
- SIEM Analytics
- The SOC, SecOps and SIEM
- Incident Response and Automation
- SIEM Buyer's Guide

CONTACT

2 Waters Park Dr., Suite 200
San Mateo, CA 94403

1.844.EXABEAM

info@exabeam.com

Terms & Privacy Policy — Sitemap