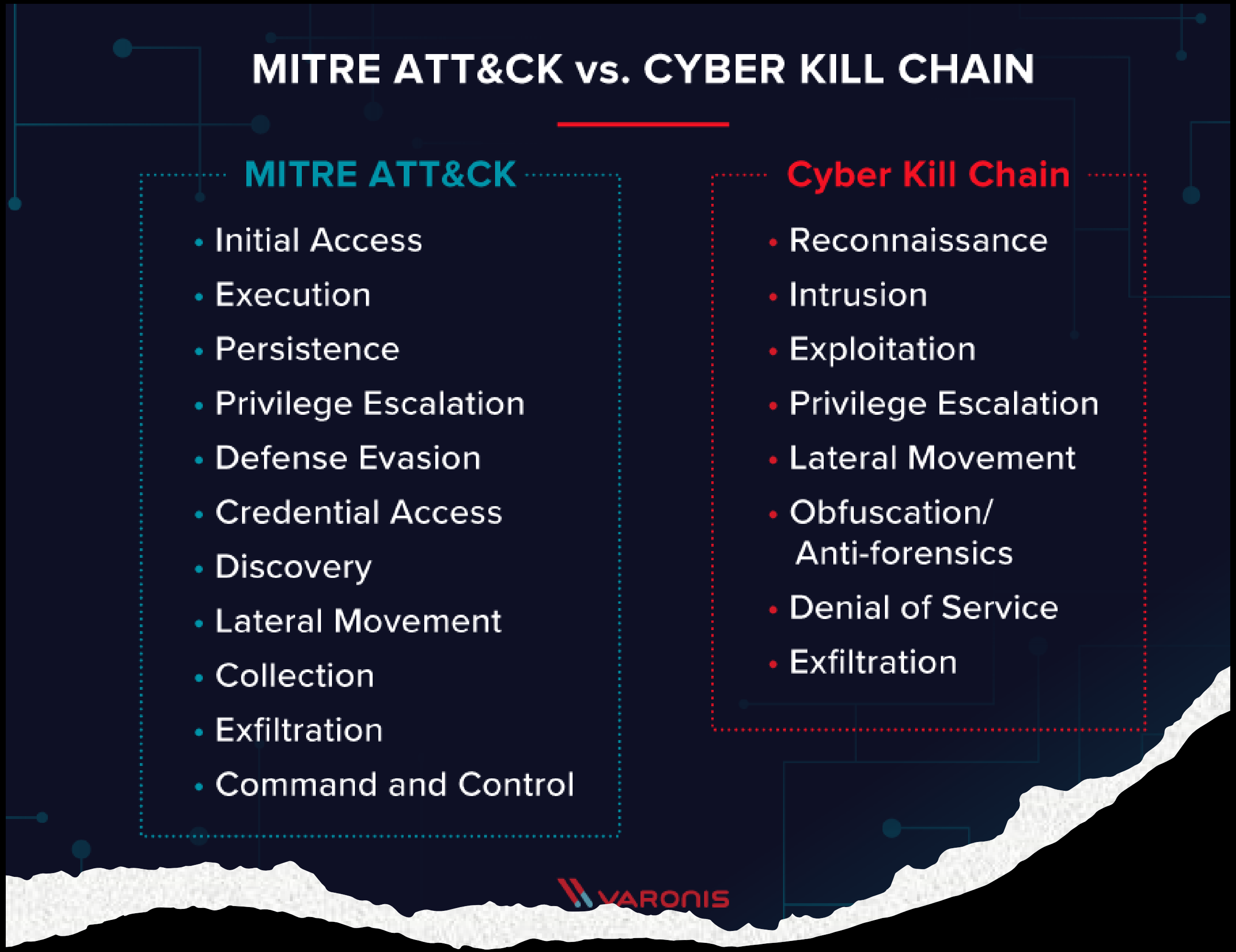
APT28: Understanding a group specializing in attacks against intelligence sectors

joas antonio

About me

- Joas Antonio;
- 20 Years/Asperger's;
- Information Security Analyst (Red team) on move;
- Researcher by Miter att&ck;
- OWASP Project Leader;
- hacking is note the Crime advocate;
- CEH Master Certifications, eJPT, eWPT, eWPTX, eMAPT and OSWP;

WHAT IS MITER ATT&CK?



MITRE ATT&CK vs. CYBER KILL CHAIN

MITRE ATT&CK

- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Exfiltration
- Command and Control

Cyber Kill Chain

- Reconnaissance
- Intrusion
- Exploitation
- Privilege Escalation
- Lateral Movement
- Obfuscation/ Anti-forensics
- Denial of Service
- Exfiltration

VARONIS

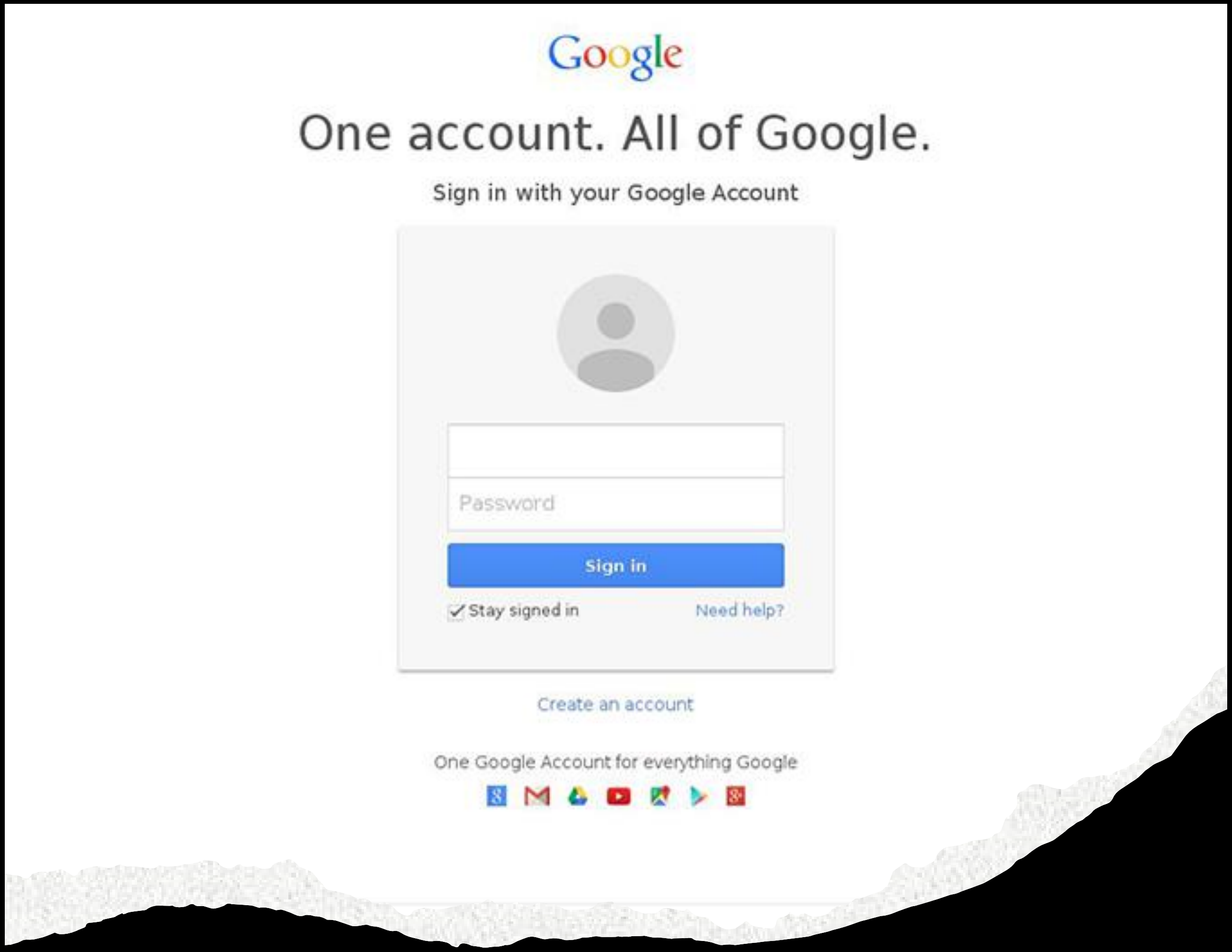
- MITER introduced ATT&CK ((Adversarial tactics, Techniques & Common knowledge–Tactics, Techniques and Common Knowledge of Opponents) in 2013 as a way to describe and categorize opponents' behaviors. ATT&CK is a structured list of known attacker behaviors that have been compiled into tactics and techniques, expressed in various matrices and also through STIX/TAXII(STIX and TAXII are standards developed with the aim of improving cyber-attack prevention and mitigation. STIX defines what threat intelligence is, while TAXII defines how that information is relayed.) Because this list is a comprehensive representation of the behaviors attackers use when compromising networks, it is useful for a variety of offensive and defensive measures, impersonations, and other mechanisms.

APT28

- IT'S a threat group that was assigned to military unit 26165 of the 85th Special Services Center (GTsSS) of the 85th Special Services Center (GTsSS) from Russia

- sreportedly compromised the Hillary Clinton campaign, the Democratic National Committee and the Democratic Congressional Campaign Committee in 2016 in an attempt to interfere in the US presidential election, associated with TG-4127.

TTPS: INVASION



Google

One account. All of Google.

Sign in with your Google Account

Spear-Phishing

- TG-4127 explored the use of Gmail by the Hillary for Americaand leveraged campaign employees' expectation of the default Gmail login page to access their email account. When presented with the fake TG-4127 login page (see Figure 1), victims may be convinced that it was the legitimate login page for their hillaryclinton.com email account.

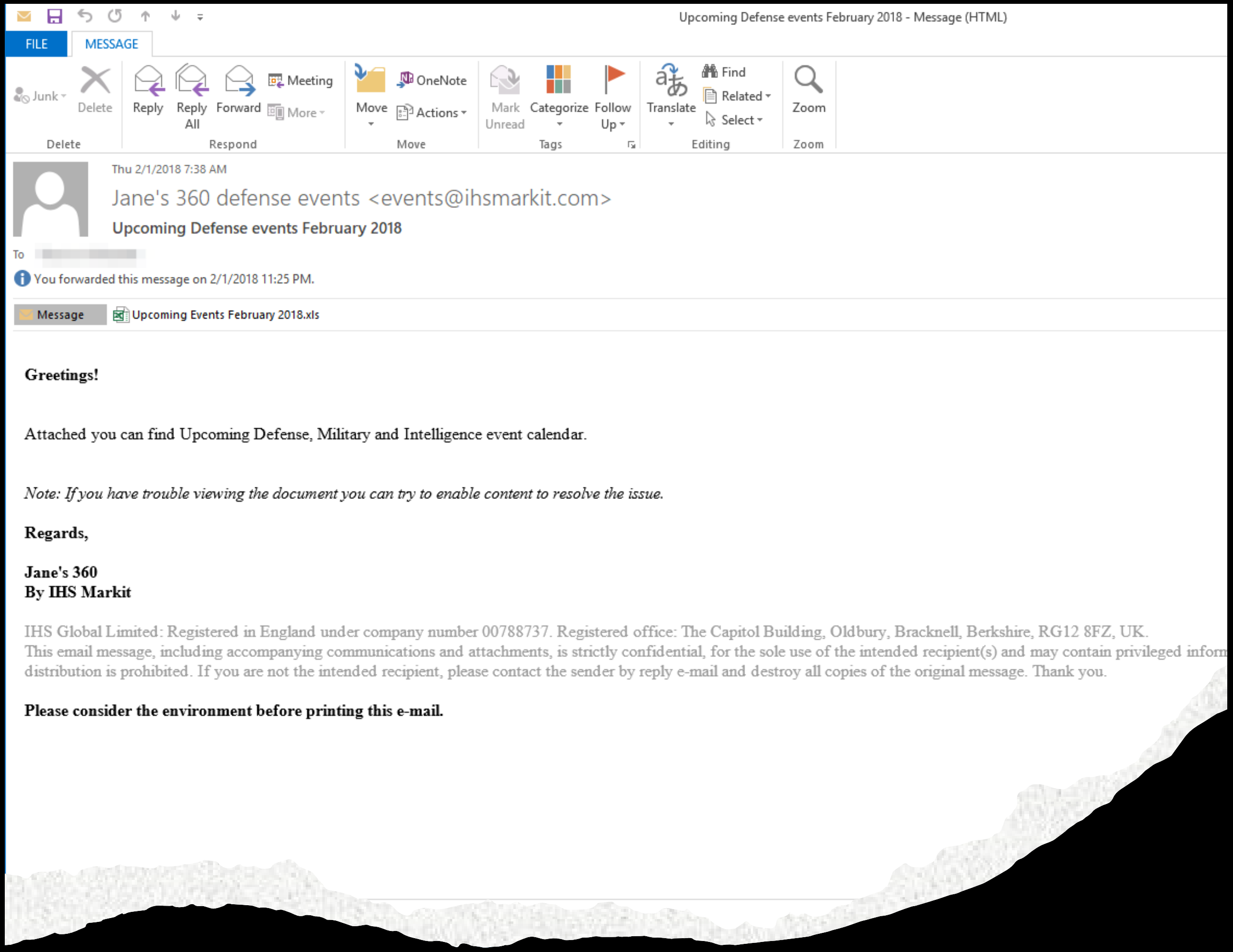
During this period, TG-4127 created 213 short links targeting 108 email addresses in the hillaryclinton.com domain. Through open source research, CTU researchers identified the owners of 66 of thespear-phishing.

- The targets had the following titles:
- national political director
- finance director
- Director of Strategic Communications
- Scheduling Director
- travel director
- Traveling press secretary
- travel coordinator

The data of bitly available publicly reveal how many short links were clicked, likely by a victim opening an email from spearphishingand clicking the link to the fake Gmail login page. Only 20 of the 213 short links have been clicked until this post. Eleven of the links were clicked once, four were clicked twice, two were clicked three times, and two were clicked four times.

Spear-Phishing with Malicious XLS

- THEattack directed at two government institutions related to foreign relations. These entities are not regionally congruent, and the only shared victimology involves their organizational functions. Specifically, one organization is geographically located in Europe and the other in North America. The initial attack vector took advantage of an email fromphishing. Analysis of the email header data showed that the sender address was spoofed and did not originate from theIHSMarkit. The bait text in the email fromphishing states that the annex is a calendar of events relevant to the targeted organizations and contained specific instructions on what actions the victim would have to take if they had “problems viewing the document”.



Upcoming Defense events February 2018 - Message (HTML)

Thu 2/1/2018 7:38 AM

Jane's 360 defense events <events@ihsmarkit.com>

Upcoming Defense events February 2018

To [redacted]

You forwarded this message on 2/1/2018 11:25 PM.

Upcoming Events February 2018.xls

Greetings!

Attached you can find Upcoming Defense, Military and Intelligence event calendar.

Note: If you have trouble viewing the document you can try to enable content to resolve the issue.

Regards,

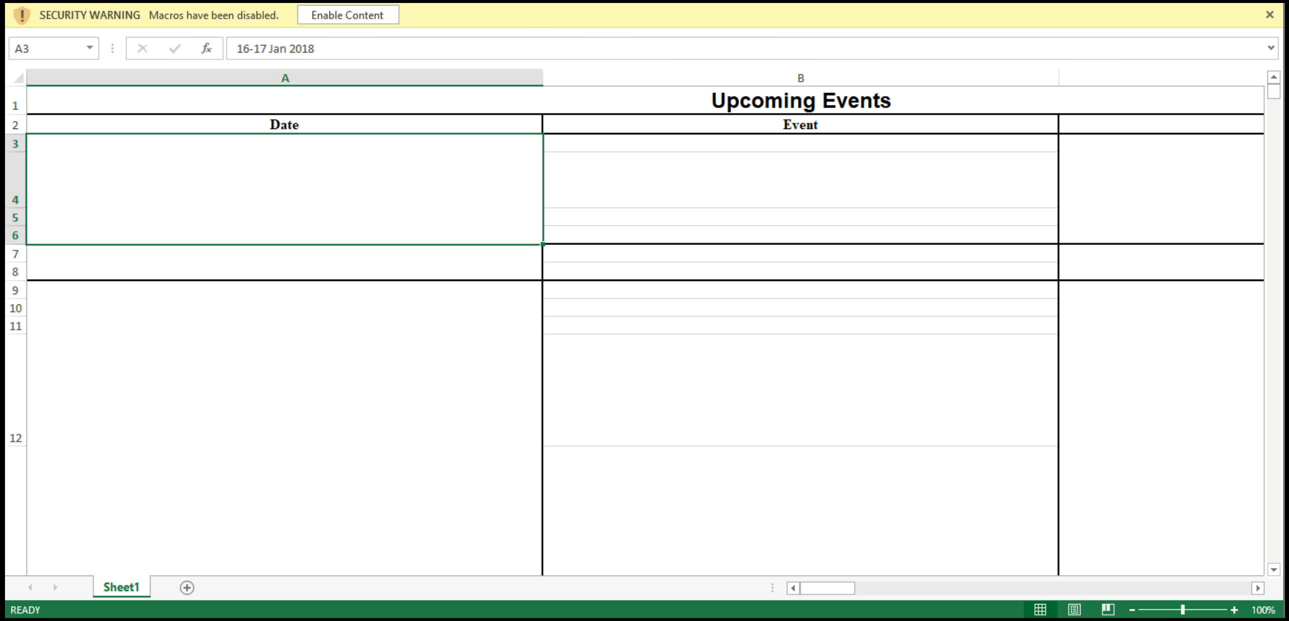
Jane's 360
By IHS Markit

IHS Global Limited: Registered in England under company number 00788737. Registered office: The Capitol Building, Oldbury, Bracknell, Berkshire, RG12 8FZ, UK.
This email message, including accompanying communications and attachments, is strictly confidential, for the sole use of the intended recipient(s) and may contain privileged inform
distribution is prohibited. If you are not the intended recipient, please contact the sender by reply e-mail and destroy all copies of the original message. Thank you.

Please consider the environment before printing this e-mail.

Spear-Phishing with Malicious XLS

- The attachment itself is a Microsoft Excel XLS document that contains malicious macro script. The document presents itself as a standard macro document, but has all its text hidden until the victim enables the macros. Notably, the entire text of the content can be accessed by the victim even before the macros are enabled. However, a white font color is applied to the text to make it appear that the victim must enable macros to access the content. Using code:`ActiveSheet.Range ("a1:c54"). Font.Color = vbBlack`
  The above code changes the font color to black within the specified cell range and presents the content to the user.



SECURITY WARNING Macros have been disabled.

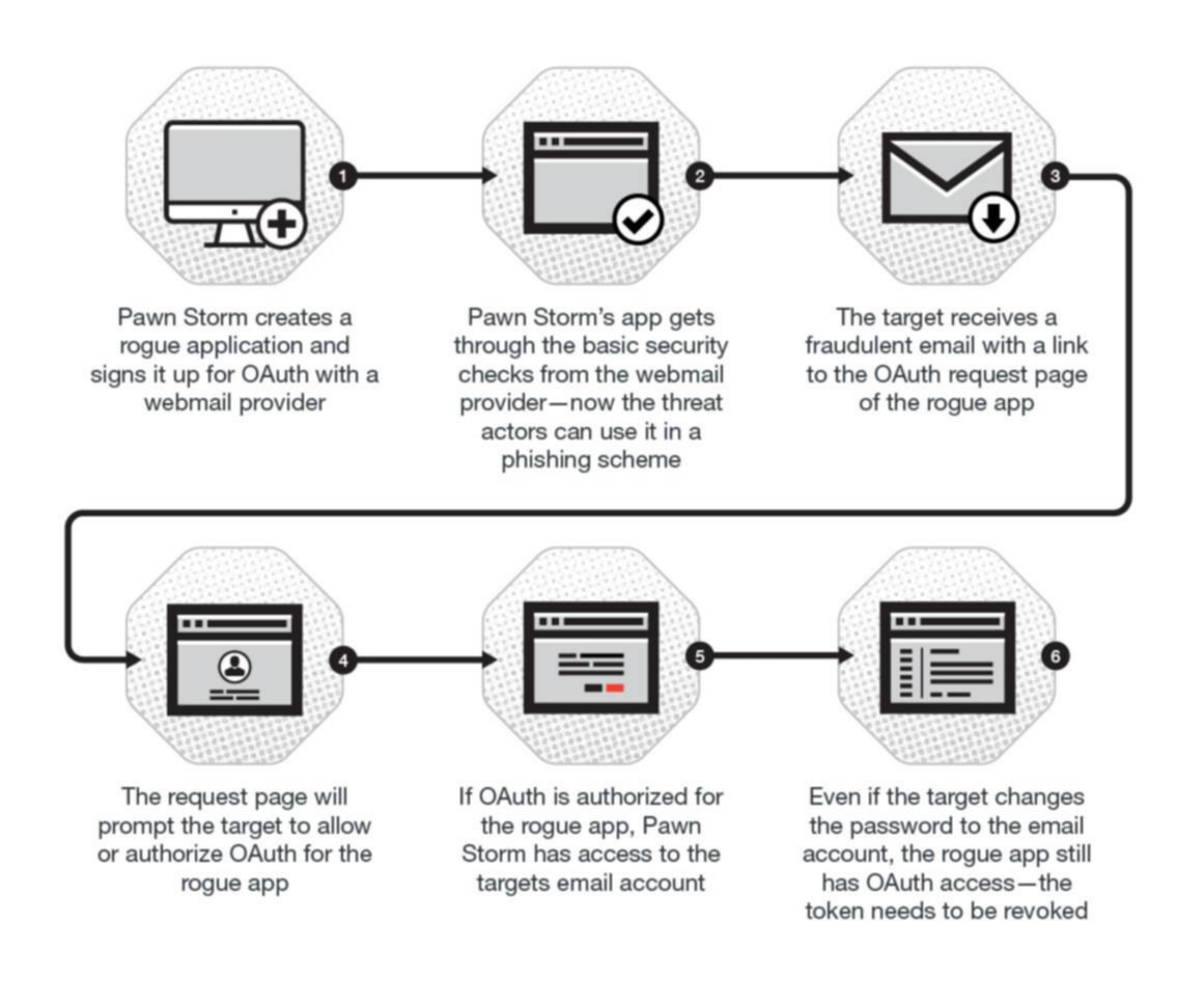
A3 16-17 Jan 2018

Upcoming Events

Date	Event

Token Theft

- pawn Storm is an active and aggressive spy group that has been operating since 2004. The group uses different methods and strategies to obtain information from its targets, which are covered in our latest research. However, they are especially known for dangerous campaigns ofphishingof credentials. In 2016, the group launched aggressive attacks ofphishing of credentials against the Democratic National Convention (DNC), the German political party Christian Democratic Union (CDU), the parliament and government of Turkey, the parliament of Montenegro, the World Anti-Doping Agency (WADA), Al Jazeera and many other organizations .



1. Pawn Storm creates a rogue application and signs it up for OAuth with a webmail provider
2. Pawn Storm's app gets through the basic security checks from the webmail provider—now the threat actors can use it in a phishing scheme
3. The target receives a fraudulent email with a link to the OAuth request page of the rogue app
4. The request page will prompt the target to allow or authorize OAuth for the rogue app
5. If OAuth is authorized for the rogue app, Pawn Storm has access to the targets email account
6. Even if the target changes the password to the email account, the rogue app still has OAuth access—the token needs to be revoked

TTPS: DEFENSE EVASION

Collected data file: file via utility

- An adversary can compress or encrypt data collected before exfiltrationusing third-party utilities. There are many utilities that can archive data, including 7-Zip,WinRAR and WinZip. Most utilities include functionality to encrypt and/or compress data.
- Some third-party utilities may be pre-installed, such as tarno Linux and macOS or zip Windows systems.
- APT28 used a variety of utilities, including WinRAR, to archive the collected data with password protection

Matching the legitimate name or location

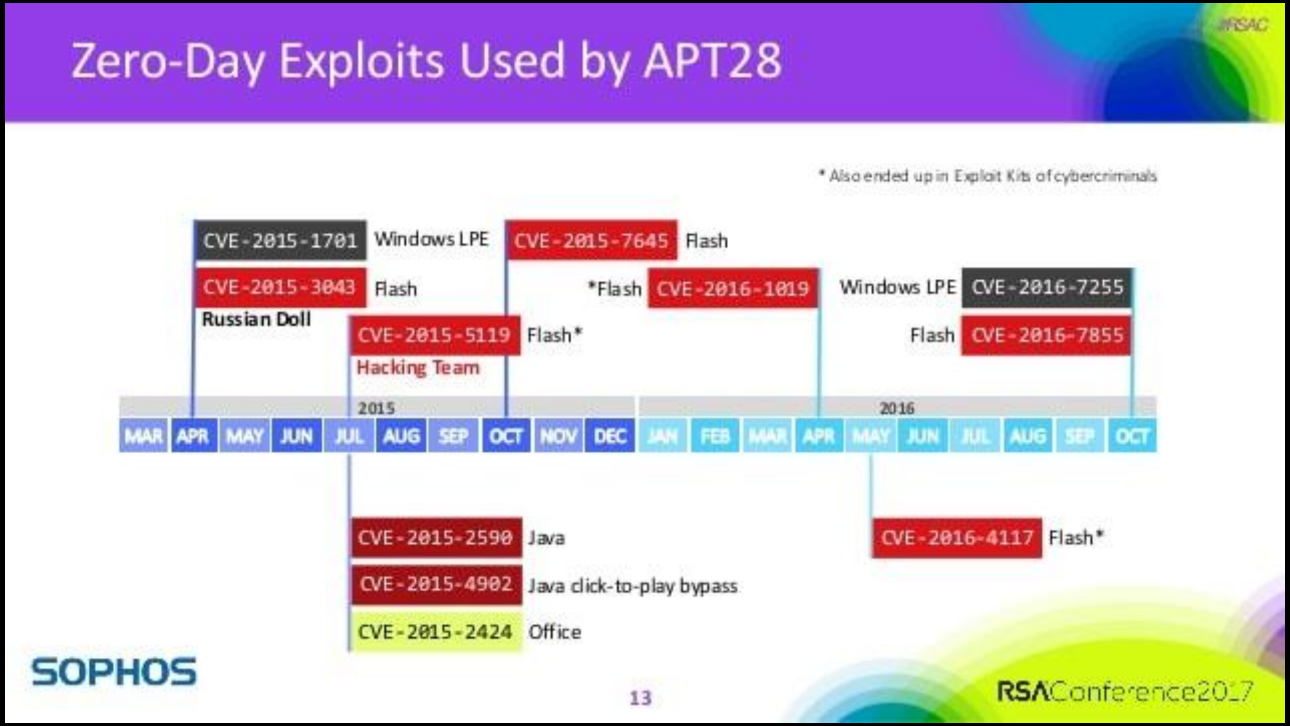
- Opponents can match or approximate the name or location of legitimate files or resources when naming/placing them. This is done to avoid defenses and observation. This can be done by placing an executable in a commonly trusted directory (eg in System32) or by giving it the name of a trusted and legitimate program (eg svchost.exe). In containerized environments, this can also be done by creating a resource in anamespace that corresponds to the naming convention of a cancontainer or cluster. Alternatively, the name of a given container file or image could be an approximation of legitimate programs/images or something innocuous.
- APT28 changed the extensions of files that contain data exfiltrates to make them look benign and renamed an instance of shell from the web to appear as a legitimate OWA page.

TTPS: SCALE OF PRIVILEGES AND SIDE HANDLING

Access Token manipulation: token impersonation/Theft

- THE FireEye labsrecently detected a limited APT campaign exploiting zero-day vulnerabilities in Adobe Flash and a new one in Microsoft Windows. Using the**dynamics Threat intelligence Cloud (DTI)** , The researchers FireEye detected a pattern of attacks initiated on April 13 th , 2015. Adobe independently patched the vulnerability (CVE-2015-3043) in **APSB15-06**. Through the correlation of technical indicators and command and control infrastructure, theFireEye assesses that APT28 is probably responsible for this activity.

1. User clicks link to attacker controlled Web site
2. HTML/JS launcher page serves Flash exploit
3. Flash exploit triggers CVE-2015-3043, run shellcode
4. shellcode downloads and runs executable payload
5. executable payload exploits place privilege escalation (CVE-2015-1701) to steal System token

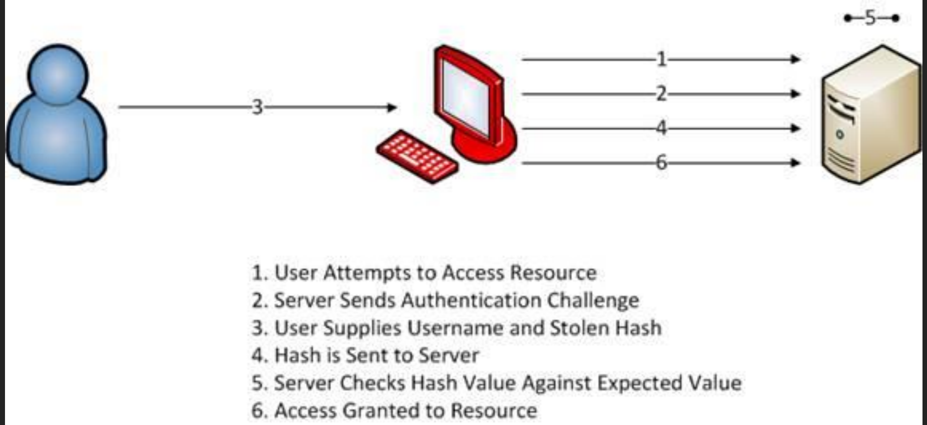


Zero-Day Exploits Used by APT28

* Also ended up in Exploit Kits of cybercriminals

Use Alternate Authentication Material: Pass the Hash

- An atack Pass-the-Hash (PtH) is a technique by which an attacker captures a hashpassword (as opposed to password characters) and then simply passes it on for authentication and potentially lateral access to other networked systems. The threat actor does not needdecrypt The hashto get a plain text password. the attacksPtH exploit the authentication protocol, as the hashof passwords remains static for each session until the password is rotated. Attackers often gethashes scraping a system's active memory and other techniques.
- although the attacks Pass-the-Hash (PtH) can occur on Linux, Unix and other platforms, they are more prevalent on Windows systems. On Windows, thePtH explore the single Sign-On (SS0) via NT Lan Manager (NTLM), Kerberosand other authentication protocols. When a password is created in Windows, it ishash and stored in the Security Accounts Manager (SAM), in the Local Security Authority Subsystem (LSASS) process memory, in the credential Manager (CredMan), in a database ntds.dit on Active directoryor elsewhere. So when a user doeslogin on a Windows workstation or server, it basically leaves your password credentials behind.



1. User Attempts to Access Resource
2. Server Sends Authentication Challenge
3. User Supplies Username and Stolen Hash
4. Hash is Sent to Server
5. Server Checks Hash Value Against Expected Value
6. Access Granted to Resource

https://www.secureworks.com/research/threat-group-4127-targets-hillary-clinton-presidential-campaign

https://unit42.paloaltonetworks.com/unit42-sofacy-attacks-multiple-government-entities/

https://www.trendmicro.com/en_us/research/17/d/pawn-storm-abuses-open-authentication-advanced-social-engineering-attacks.html

https://media.defense.gov/2021/Jul/01/2002753896/-1/-1/1/CSA_GRU_GLOBAL_BRUTE_FORCE_CAMPAIGN_UOO158036-21.PDF

https://staylocksec.com/2021/03/05/pass-the-hash/

https://attack.mitre.org/groups/G0007/

https://mitre-attack.github.io/attack-navigator//#layerURL=https%3A%2F%2Fattack.mitre.org%2Fgroups%2FG0007%2FG0007-enterprise-layer.json