Pawn Storm Ramps Up Spear-phishing Before Zero-Days Get Patched

Posted on: November 9, 2016 at 5:00 am **Posted in:** Exploits, Targeted Attacks, Vulnerabilities
Author: Trend Micro

by Feike Hacquebord and Stephen Hilt

The effectiveness of a zero-day quickly deteriorates as an attack tool after it gets discovered and patched by the affected software vendors. Within the time between the discovery of the vulnerability and the release of the fix, a bad actor might try to get the most out of his previously valuable attack assets. This is exactly what we saw in late October and early November 2016, when the espionage group Pawn Storm (also known as Fancy Bear, APT28, Sofacy, and STRONTIUM) ramped up its spear-phishing campaigns against various governments and embassies around the world. In these campaigns, Pawn Storm used a previously unknown zero-day in Adobe's Flash (CVE-2016-7855, fixed on October 26, 2016 with an emergency update) in combination with a privilege escalation in Microsoft's Windows Operating System (CVE-2016-7255) that was fixed on November 8, 2016.

After the fix of CVE-2016-7855 in Adobe's Flash, Pawn Storm probably devalued the two zero-days in its attack tool portfolio. Instead of only using it against very high profile targets, they started to expose much more targets to these vulnerabilities. We saw several campaigns against still-high-profile targets since October 28 until early November, 2016.

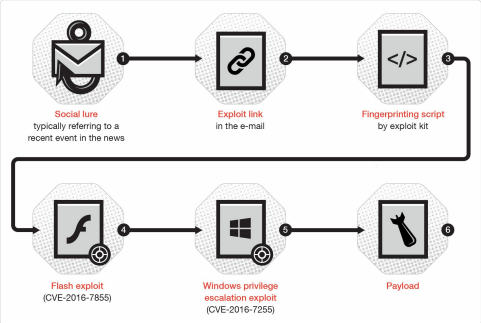


Figure 1. Infection chain of the spear-phishing campaign

In early November, Pawn Storm sent spear-phishing e-mails to various governments around the world. In one of Pawn Storm's campaigns on November 1, the subject line was "European Parliament statement on nuclear threats." The e-mail seemingly came from a real press officer working for the media relations office of the European Union, but in reality, the sender e-mail address was forged. Clicking on the link in the spear-phishing e-mail led to the exploit kit of Pawn Storm.

The exploit kit will first fingerprint its targets with invasive JavaScript, which uploads OS details, time zone, installed browser plugins, and language settings to the exploit server. The exploit server may then send back an exploit or simply redirect to a benign server. In recent attacks, we observed that the exploit kit exposed selected targets to the Flash vulnerability CVE-2016-7855, combined with the then-unpatched privilege escalation vulnerability in Windows (CVE-2016-7255). Internet users who were using Windows Vista up to Windows 7 without the latest patch for Flash would be at high risk of automatically getting infected.

From October 28 until early November 2016, several waves of spear-phishing e-mails were sent to embassies and other governmental institutions. Some of the e-mails posed as an invitation for a "Cyber Threat Intelligence and Incident Response conference in November" by Defense IQ, a media organization that specializes in news on defense and the military. The conference is real, but of course, the sender address was forged. The spear-phishing e-mail contained an RTF (Rich Text Format) document called "Programm Details.doc."

Opening the RTF document (detected by Trend Micro as TROJ_ARTIEF.JEJOSU) would show the program details of the real conference, which was to be held in London in late November 2016. However, the RTF document has an embedded Flash file (SWF_CONEX.A) that downloads additional files from a remote server. This attack methodology of Pawn Storm has been previously observed. We also noted that the embedded Flash file downloaded a Flash exploit for the just-patched CVE-2016-7855. A second file was also downloaded, but this file consistently crashed Microsoft Word during our tests.

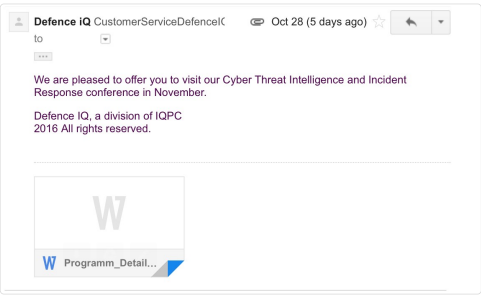


Figure 2. Spear-phishing e-mail from Pawn Storm

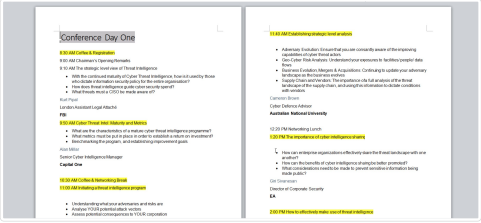
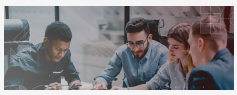


Figure 3. The Word document with an embedded Flash file that will try to download exploits from a remote server. The program was taken from a real conference to be held in London in end of November.

Apart from these two campaigns, several others were also launched by Pawn Storm in the period between the discovery of the zero-days and the release of Adobe's and Microsoft's patches on October 26 and November 8, 2016. This shows that Pawn Storm ramped up their spear-phishing attacks shortly after its zero-days were discovered. Not all organizations may have been able to immediately patch Adobe's Flash, and the Windows vulnerability wasn't patched until November 8,

Security Predictions for 2020



Cybersecurity in 2020 will be viewed through many lenses — from differing attacker motivations and cybercriminal arsenal to technological developments and global threat intelligence — only so defenders can keep up with the broad range of threats.
Read our security predictions for 2020.

Business Process Compromise

Attackers are starting to invest in long-term operations that target specific processes enterprises rely on. They scout for vulnerable practices, susceptible systems and operational loopholes that they can leverage or abuse. To learn more, read our Security 101: Business Process Compromise.

Recent Posts

- OpenSMTPD Vulnerability (CVE-2020-8794) Can Lead to Root Privilege Escalation and Remote Code Execution
- Operation Overtrap Targets Japanese Online Banking Users Via Bottle Exploit Kit and Brand-New Cinobi Banking Trojan
- March Patch Tuesday: LNK, Microsoft Word Vulnerabilities Get Fixes, SMBv3 Patch Follows
- Busting Ghostcat: An Analysis of the Apache Tomcat Vulnerability (CVE-2020-1938 and CNVD-2020-10487)
- Dissecting Geost: Exposing the Anatomy of the Android Trojan Targeting Russian Banks

Popular Posts

- LokiBot Impersonates Popular Game Launcher and Drops Compiled C# Code File
- Misconfigured Container Abused to Deliver Cryptocurrency-mining Malware
- Dissecting Geost: Exposing the Anatomy of the Android Trojan Targeting Russian Banks
- February Patch Tuesday: Fixes for Critical LNK, RDP, Trident Vulnerabilities
- Outlaw Updates Kit to Kill Older Miner Versions, Targets More Systems

Stay Updated

Email Subscription
Your email here
Subscribe

2016.

End users are urged to update their Windows OS (through MS16-135), and Flash Player (via its emergency patch) to mitigate these threats.

Trend Micro Solutions

Trend Micro™ Deep Discovery™ provides detection, in-depth analysis, and proactive response to today's stealthy malware, and targeted attacks in real-time. It provides a comprehensive defense tailored to protect organizations against targeted attacks and advanced threats through specialized engines, custom sandboxing, and seamless correlation across the entire attack lifecycle, allowing it to detect threats like the above mentioned zero-day attacks even without any engine or pattern update.

Trend Micro™ Deep Security™ and Vulnerability Protection provide virtual patching that protects endpoints from threats that abuses unpatched vulnerabilities. OfficeScan's Vulnerability Protection shield endpoints from identified and unknown vulnerability exploits even before patches are deployed.

TippingPoint customers are protected from attacks exploiting these vulnerabilities with these MainlineDV filters:

- 25498: HTTP: Adobe Flash AMF Use-After-Free Vulnerability
- 25729: HTTP: Microsoft Windows NtSetWindowLongPtr Privilege Escalation Vulnerability
- 25728: HTTPS: TROJ_KEFLER.A Checkin
- 25718: HTTP: Microsoft Windows Privilege Escalation Vulnerability

Trend Micro™ Deep Security™ and Vulnerability Protection shield endpoints and networks through Rule update DSRU16-034, which includes these Deep Packet Inspection (DPI) rules:

- 1008003-Adobe Flash Player Use-After-Free Vulnerability (CVE-2016-7855)
- 1008033-Microsoft Windows Elevation Of Privilege Vulnerability
- 1008034-Microsoft Windows Multiple Security Vulnerabilities (MS16-135)

Indicators of Compromise:

Exploit sites:

- abc24news[.]com
- defenceglobalnews[.]com
- globaldefencetalk[.]com
- politlco[.]com
- pressservices[.]net
- washingtnpostnews[.]com
- worldpressjournal[.]com
- worldpostjournal[.]com

RTF document (TROJ_ARTIEF.JEJOSU): 4173b29a251cd9c1cab135f67cb60acab4ace0c5

CVE-2016-7855 sample (SWF_EXES.A): cb1e30e6e583178f8d4bf6a487a399bd341c0cdc

Payload (TSPY_SEDNIT.F): c2f8ea43f0599444d0f6334fc6634082fdd4a69f

C&C Servers:

- microsoftstoreservice[.]com
- servicetlnt[.]net
- windowsdefltr[.]net

Remote sites giving back exploits to RTF Documents with embedded SWF:

- appexsrv[.]net
- securityprotectingcorp[.]com
- uniquecorpind[.]com
- versiontask[.]com

With additional analysis by Francis Antazo and Jeanne Jocson

Update as of November 10, 2016, 2:00 AM (UTC-8):

We updated to include additional rules in TippingPoint's MainlineDV filters and Trend Micro™ Deep Security™ and Vulnerability Protection Deep Packet Inspection that address the vulnerabilities.

Tags: Adobe zero-day exploit | Pawn Storm | spear-phishing email | Windows zero-day exploit