Cyberespionage Group Turla Deploys Backdoor Ahead of G20 Task Force Summit

trendmicro.com/vinfo/vn/security/news/cyber-attacks/cyberespionage-group-turla-deploys-backdoor-ahead-of-g20-summit

A cyberespionage group known as Turla is reportedly targeting invitees, guests, and nation-state participants of the upcoming G20 task force summit in Hamburg, Germany with a backdoor named KopiLuwak (detected by Trend Micro as TROJ_KOPILUWAK.A, JS_KOPILUWAK.A, and JS_KOPILUWAK.B). The payload is capable of exfiltrating data, as well as downloading and triggering additional malware and executing arbitrary commands on the infected machine. Security researchers have since notified CERT-Bund, Germany's federal computer emergency response team.

[READ: What is spear-phishing, and how can you defend against it?]

Turla's latest campaign is noted for possibly using watering hole and spear-phishing emails that lure would-be victims with an email containing an invitation for a G20 Task Force summit on digital economy. The event is real, slated in October, and security experts note that the PDF, named *Save the Date G20 Digital Economy Taskforce 23 24 October.pdf*, attached in the spear-phishing emails appear to be a legitimate file but ultimately a decoy. It also drops a malicious JavaScript file that executes KopiLuwak in the infected system's memory when decrypted.

[RELATED: APT10/menuPass cyberespionage campaign Operation Cloud Hopper attacks managed service providers]

Turla, a Russian-speaking cyberespionage group, is known for using unique, stealthy tactics. They made headlines in early June when their command and control (C&C) servers were found hiding in the comment section of Britney Spears' Instagram posts. The malware they delivered posed as a security extension/plug-in for Firefox and distributed via a compromised Swiss website. In September 2015, they were able to conceal their C&C servers by exploiting and abusing poorly secured satellite-based internet services. In December 2014, the cyberespionage group employed an open-source backdoor that targeted machines running the Linux operating system (OS).

[From TrendLabs Security Intelligence Blog: Pawn Storm ramps up spear-phishing campaign before zero-days get patched]

The attack chain of Turla's latest campaign resembles one employed by other cyberespionage groups Pawn Storm and ChessMaster. Real events and legitimate documents were used as decoys to install backdoors on the machines of their targets of interest. This enables them to move laterally within the compromised network as well as steal confidential and mission-critical data.

These cyberespionage attacks highlight the need for organizations to be similarly proactive in order to prevent intrusion or mitigate their effects. IT/system administrators and information security professionals should adopt best practices against targeted attacks. Keeping the OS and its programs updated should be intuitive—it helps prevent attackers from leveraging security flaws as doorways into the systems. Consider virtual patching in the absence of patches for certain vulnerabilities. Enforce the principle of least privilege. Secure your email gateways and, more importantly, implement defense in depth—multilayered security mechanisms—to protect the security, integrity, and availability of your organization's important assets.

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 those employed by cyberespionage group Turla, even without any engine or pattern update.

Trend Micro's Hybrid Cloud Security solution, powered by XGen™ security and features Trend Micro™ Deep Security™, delivers a blend of cross-generational threat defense techniques that have been optimized to protect physical, virtual, and cloud workloads/servers.

HIDE

Like it? Add this infographic to your site:
1. Click on the box below.   2. Press Ctrl+A to select all.   3. Press Ctrl+C to copy.   4. Paste the code into your page (Ctrl+V).

Image will appear the same size as you see above.

Posted in Cyber Attacks, phishing