Create a Solid Line of Defense against Pawn Storm and Similar Threats

Pawn Storm has been a recognized campaign since 2004, when we first detected activity from this particular threat actor group. Their continued operations, specifically over the past two years, show that they have ample resources, effective strategies, and clear objectives. Recently, the group has focused on obtaining information and strategically releasing details to manipulate certain events, influence mainstream media, and even change public opinion. While this may seem confined to the political sphere, average citizens can fall victim to their widespread cyber propaganda operations. Other threat actors can also easily adopt their methodologies or repurpose them for different goals, such as corporate espionage or influencing public opinion on organizations and products.

Since the group has been active for many years, their methods of attack are well-documented: from using sophisticated social engineering lures, efficient credential phishing campaigns, and potent zero-days, to leveraging a private exploit kit with an effective set of malware and conducting false flag operations. Specific tactics are used for specific targets, and the threat actors behind Pawn Storm have the resources and tools for prolonged operations.

Understanding the ways Pawn Storm compromises its targets can help organizations create a solid line of defense and protect themselves against this and similar campaigns.

PROTECTION AGAINST PHISHING

Phishing is one of the oldest scams on the internet, yet its continued prevalence shows that attackers are adapting and still turning a profit. Effective phishing campaigns were the main source of Pawn Storm's information. The group uses sophisticated tactics like tabnabbing, creating Enterprise Outlook Web Access (OWA) phishing login pages, and Open Authentication (OAuth) abuse. They also have the resources to maintain long-running campaigns.

Because of the nature of this threat, a multilayered approach is essential for protecting employees and their organizations. Trend Micro offers a wide range of solutions that protect enterprises across gateways, endpoints, networks, and servers, including:

- Trend Micro™ InterScan™ Web Security, a virtual appliance or a cloud-based service that protects against cyber threats at the internet gateway with Advanced Persistent Threat (APT) detection, real-time web reputation, and URL filtering. This tool blocks user access to malicious URLs that are part of elaborate phishing scams. It can be integrated into the Trend Micro Deep Discovery™ Analyzer, which features a sandbox analysis capability for optimized protection. InterScan Web Security also:
  - Prevents drive-by downloads, tabnabbing and blocks access to spyware and phishing-related websites
  - Utilizes six different policy actions for web access control, including: monitor, allow, warn, block, block with password override, enforce time quota
  - Employs object-level blocking within dynamic web pages such as Web 2.0 mashups
  - Detects and blocks access to command and control servers

- Enterprises can also use Trend Micro Deep Discovery Email Inspector, which detects most spear-phishing attacks using password derivation for zipped and protected files, as well as document exploit detection and sandboxing to accurately find malicious attachments. It also uses embedded URL analysis via sandboxing, reputation and page analysis to spot links leading to malicious sites.

- To secure endpoints, the Trend Micro Smart Protection Suites provide comprehensive protection for all devices, including mobile devices and other endpoints, against advanced threats that traditional solutions cannot detect. Smart Protection Suites integrates features that are an effective countermeasure against spam, phishing and APTs:

    - Trend Micro InterScan Messaging Security protects against both traditional and targeted attacks. It can detect socially engineered email threats like phishing and spearphishing and has features that include sandbox analysis of suspicious attachments and detection of malicious embedded URLs.

- The Smart Protection Suites are powered by XGen™ Endpoint Security, which has a high-fidelity machine learning feature that conducts pre-execution and run-time analysis along with behavior analysis. Its other technologies include:

    - Web and file reputation technologies detect and block access to malicious files

    - Exploit prevention blocks access to exploit kits that may lead to compromise

    - Application control allows only safe files to run on systems and networks

    - Variant protection

PROTECTION AGAINST NETWORK INTRUSION

Pawn Storm uses command-and-control (C&C) servers across multiple countries to communicate with compromised systems, relay information, and deploy their attacks. Our researchers have been tracking the group's second stage C&C servers since 2013, which gives us unique insight into their operations.

- Trend Micro Deep Discovery Inspector prevents these scenarios from taking place by monitoring network traffic, C&C communications, encryption behaviors, and zero-day exploitation via:

    - Custom sandboxing

    - An extensive array of detection techniques across multiple ports and protocols

    - Threat actor behavior analysis

- Trend Micro Deep Security™ has a virtual patching feature that keeps servers, systems, and software updated. In the absence of security updates (as in zero-day attacks), virtual patching comes in handy. Business-critical services that need to stay up and running even through patch deployment, which can cause system downtime and disrupt operations will not be affected.

PROTECTION AGAINST DNS SETTINGS COMPROMISE

Pawn Storm compromises corporate email systems by changing their DNS settings to point to a proxy server and intercepting incoming emails. This particular attack scenario is not unique—quite a few reputable companies have had their DNS settings compromised in the past by hackers that were looking for attention or promoting a cause.

Trend Micro provides an efficient solution that organizations can rely on to safeguard enterprise email servers:

- Trend Micro Deep Security protects critical enterprise applications and data from breaches and business disruptions. Corporate mail servers are secure with its application control and integrity monitoring features that detect or block the modification of their MX records from within the HOSTS file.

PROTECTION AGAINST EXPLOITS AND VULNERABILITIES

Pawn Storm exploits zero-day vulnerabilities, such as those in Adobe and Microsoft, in tandem when they identify a worthwhile target. Their initial compromise is a scouting mission, and if they find a valuable victim then they deploy more serious tools from their arsenal. One of their preferred methods of deploying exploits is using watering hole attacks— compromising websites and linking targets to the group's private exploit kit.

Trend Micro virtual patching and threat protection technologies in the following solutions can stop exploits from affecting software and applications:

- Trend Micro Smart Protection Suites detects and blocks advanced malware and exploit kits. Its vulnerability shielding component can prevent exploits from using security bugs as an infection vector. And apart from exploit prevention, the Trend Micro Smart Protection Suites with XGen Endpoint Security also combines machine learning, which employs pre-execution and run-time analysis with behavioral analysis, and file reputation technology to detect exploits.
- XGen Endpoint Security's machine learning mechanism performs static and dynamic analyses on files that are executed on systems. At the gateway level, its exploit prevention feature blocks exploit kits that come with other malware.
- Trend Micro Deep Security has a vulnerability-shielding mechanism that secures software and applications from known exploits.
- TippingPoint® NextGeneration Intrusion Prevention System (NGIPS) is a comprehensive and contextual awareness network traffic solution for advanced threats that exploit vulnerabilities with features that include:
    - Threat intelligence from sources such as Digital Vaccine Labs (DVLabs) and the Zero-Day Initiative (ZDI) along with vulnerability information from the Common Vulnerabilities and Exposures (CVE) database, to ensure broad vulnerability exploitation coverage.
    - Virtual patching to shield vulnerabilities against exploits
    - Machine learning technology to detect exploit kits

Securing Your Journey to the Cloud