A **TrendLabs** Security in Context Paper

TREND MICRO™

The Enterprise Fights Back (Part II)

Protecting Sensitive Data from Targeted Attacks

How Threat Actors Steal Your Data

Data exfiltration is the final stage of a targeted attack campaign where threat actors steal valuable corporate information while remaining undetected.[1]

Threat actors use a variety of legitimate and malicious tools to extract specific information and mimic normal network traffic. For instance, the EvilGrab malware, which is related to a targeted attack campaign, uses a Windows filter to grab audio and video files.[2] Other techniques include using backdoor malware to upload gathered files, file transfer protocol (FTP) to transfer files without consent, and WMI (Windows Management Instrumentation) to monitor and capture recently opened files, and web applications to open browsers.

43%

of most serious threats to the company's enterprise IT infrastructure are from external sources.

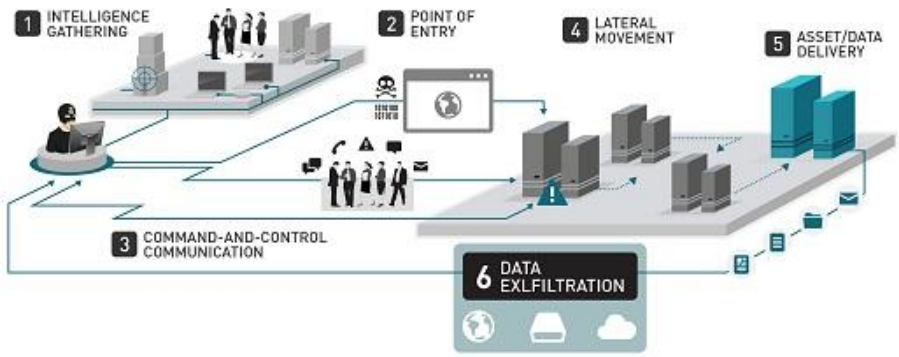

Figure 1: Targeted Attack Campaign Diagram

Preventing the exposure of confidential information is a top challenge for most (71%) enterprises.[3] Given the introduction of the mobile platform and the sophistication of targeted attacks, enterprises need to step up to protect its intellectual property, trade secrets, and other sensitive information.

---

[1] Trend Micro Incorporated. *A TrendLabs Security in Context Paper*. "Data Exfiltration: How Do Threat Actors Steal Your Data?" Last updated on: September 2013. Accessed on: November 2013. http://about-threats.trendmicro.com/cloud-content/us/ent-primers/pdf/how_do_threat_actors_steal_your_data.pdf

[2] Trend Micro Incorporated. *A TrendLabs Report*. "2Q Report on Targeted Attack Campaigns". Last updated on: July 2013. Accessed on: November 2013. http://about-threats.trendmicro.com/cloud-content/us/ent-primers/pdf/2q-report-on-targeted-attack-campaigns.pdf

[3] International Data Corporation. *An IDC Infographic Sponsored by Trend Micro*. "Keeping Corporate Data Safe". Last updated on: 2013. Accessed on: November 2013. http://apac.trendmicro.com/apac/enterprise/security-suite-solutions/esdp-suite/infographic/index.html

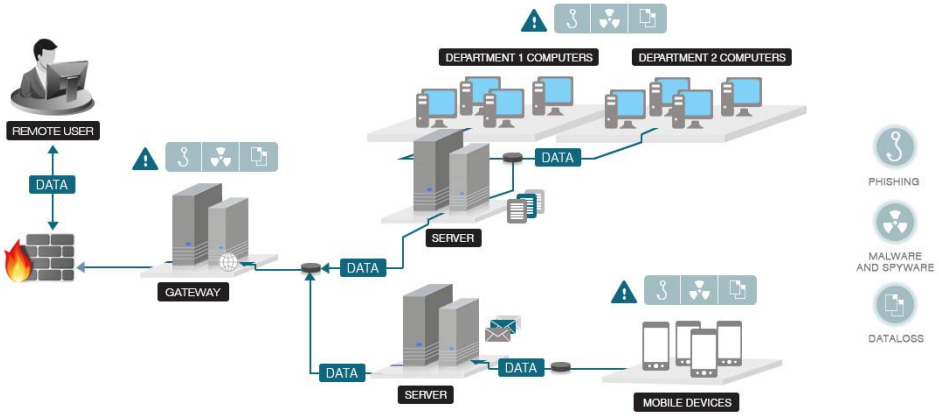

Figure 2: Potential Data Threats in an Enterprise Network

The Risks of Unprotected Data

Data breach and data loss are the most obvious outcomes of a successful targeted attack. However, the following shows real-world consequences that come right after:

Incident Responses and Crisis Management Costs

These include all the monetary costs and resources needed for a company to gauge the amount of damage, find the nature of data stolen, and track all possible traces of the attack.

Compliance-Related Penalties

These involve fines incurred by organizations following strict regulations, as those running industrial control systems (ICS).

Intangible Sunk Costs

This is the amount that organizations already invested into intangible assets such as research and development advances and trade secrets, the theft of which can decrease their competitive advantage.

Damage to Industry Reputation

Data theft from a trusted organization can easily translate to decrease in confidence from the industry it belongs.

How to Protect Sensitive Data

Detecting targeted attacks at the data exfiltration stage is very challenging for enterprises. We recommend that enterprises assume compromise, enforce preventive measures, and use an airtight custom defense strategy that can detect threats in real time. We have stressed that securing the network infrastructure is the first step in the fight against targeted attacks.[4] This time, we present these key points as the next vital step: protecting valuable data[5]:

Classify "Crown Jewels" from Normal Data

Every department or business unit should classify the crown jewels, the release of which can negatively affect an organization, from normal day-to-day documentation. These include government information, scientific research, and pharmaceutical formulas. Sharing and downloading them must require privileged access. They can be spread across the network to prevent threat actors from getting the whole information.

Establish Endpoint-to-Cloud Protection

PCs, mobile devices, and removable devices should be secured by encrypting files, disk, and removable media. Identity-based encryption solutions can be used to protect emails. Data should also be encrypted when using cloud applications, public or private cloud infrastructure, and virtual environments.

Build a Data Protection Infrastructure

A protected infrastructure requires multi-tiered access, where top-level information pieces are in a disconnected network, second-level ones require a special two-factor authentication process, while third-level ones are on regular file servers.

---

[4] Trend Micro Incorporated. *A TrendLabs Security in Context Paper*. "Securing Your Network Infrastructure Against Targeted Attacks". Last updated on: 2013. Accessed on: November 2013.http://about-threats.trendmicro.com/cloud-content/us/ent-primers/pdf/the-enterprise-fights-back-p01.pdf

[5] Trend Micro Incorporated. *A Trend Micro Research Paper*. "Suggestions to Help Companies with the Fight Against Targeted Attacks". Last updated on: 2013. Accessed on: November 2013. http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-suggestions-to-help-companies-with-the-fight-against-targeted-attacks.pdf

Created by:

TrendLabs

Global Technical Support & R&D Center of TREND MICRO

Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Our innovative security solutions for consumers, businesses and governments protect information on mobile devices, endpoints, gateways, servers and the cloud. For more information, visit www.trendmicro.com

TREND MICRO™

Securing Your Journey to the Cloud