A **TrendLabs** Security in Context Paper

TREND MICRO

The Enterprise Fights Back (Part IV): Building Threat Intelligence

Indicators of Compromise

Preventing the exposure of confidential company data or "crown jewels" has been identified as a top challenge among enterprises and large organizations.[1] Threats such as targeted attacks will continue to affect them since threat actors will always target information.[2]

"Once attackers get in to a network, the organization will race against time. The longer the attackers stay in a network, the more footholds they gain and information they can steal."

—Jim Gogolinski, Trend Micro senior threat researcher

Targeted attack campaigns can have different end goals, depending on the threat actors behind them. However, they are often conducted in order to exfiltrate data from a target network. This category of threats tend to stay hidden in networks for long periods of time, laterally moving across systems and servers to close in on valuable information. This does not, however, mean that threat actors cannot try to become aggressive if the information they are after is somehow time-sensitive.

Even though targeted attacks are difficult to detect in a network, traces and clues can be found that serve as indicators of ongoing attacks or similar attacks in the future. As such, it is highly critical for enterprises to build their own threat intelligence, which they can incorporate in their security infrastructure in order to mitigate risks targeted attacks pose.

Publicly available reports on known targeted attacks are useful in identifying some indicators of compromise together with other IT sources such as data feeds and reports. Here are some examples of tokens that have been used in the past to identify the existence of a threat inside a network.

Location of Indicator	Indicator of Compromise
"Computer" in stages 1 and 2 of Figure 1	• Registry changes • File changes (e.g., name, full path, hash, size, etc.) • Event log entries • Service changes (i.e., additions and modifications) • Mutexes
Network communications, including command and control (C&C), lateral movement, and data exfiltration activities as shown in stages 3–6 in Figure 1	Incoming and outbound network traffic indicators of known publicly reported indicators of compromise such as: • URLs related to watering hole attacks • Consistent and specific URL paths

1 Trend Micro Incorporated. (2013). "Keeping Corporate Data Safe." Last accessed February 17, 2014, http://apac.trendmicro.com/apac/enterprise/security-suite-solutions/esdp-suite/infographic/index.html.

2 Trend Micro Incorporated. (2013). "Blurring Boundaries: Trend Micro Security Predictions for 2014 and Beyond." Last accessed March 4, 2014, http://about-threats.trendmicro.com/us/security-predictions/2014/blurring-boundaries/.

Location of Indicator	Indicator of Compromise
	• Packet headers • Identifiable network communication patterns • Use of unusual ports and protocols

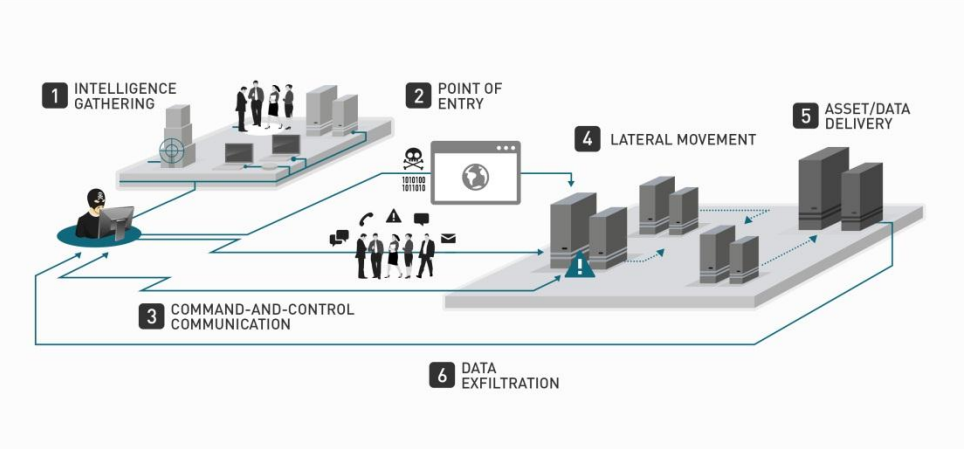

Figure 1: Stages of a targeted attack

Leveraging Threat Information

Despite the use of new malware or executable files, targeted attack campaigns may be detected early on via network traffic indicators because C&C protocols tend to remain consistent. These are more arduous to modify compared with the malware used.[3]

Publicized campaigns such as GhostNet and Nitro used malware with consistent indicators. As such, they could have been detected early on by checking and analyzing the network traffic the related malware generated. Since information on these was collated and shared across industries, threat intelligence programs can collect and correlate and pass along available data to security groups for incorporation into active defense solutions. The following are some real-world examples of how certain past attack indicators can still be used to identify possible infiltration into enterprise networks:

- Sykipot, which targeted U.S. Department of Defense smartcards, used HTTP early on to communicate with its C&C server, thus making it detectable. Older versions of Sykipot communicated via

[3] Nart Villeneuve and James Bennett. (2012). "Detecting APT Activity with Network Traffic Analysis." Last accessed March 4, 2014, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-detecting-apt-activity-with-network-traffic-analysis.pdf.

HTTPS but were still detectable because of their use of certain elements in Secure Sockets Layer (SSL) certificates.

- Enfal or Lurid had several versions that could be detected based on the way they communicated with their C&C server.[4] Even though they employed different URL paths and used commands embedded in files, they could still be detected due to their use of a specific format.

- IXESHE, which communicated over HTTP, followed a specific format and used ports 80, 8080, and 443 when they communicated with their C&C servers.[5]

- The Taidoor campaign has been using the same network traffic indicator since 2008. The related malware use three ports and communicate over HTTP.[6]

Why Building Threat Intelligence Is Crucial for Enterprises

Threat intelligence refers to any information pertaining to the tools, tactics, and procedures (TTPs) attackers use to carry out campaigns.[7] Security analysts and researchers can learn how threat actors operate and monitor ongoing campaigns via technical indicators and available information.

Through good threat intelligence, targeted attacks can be detected earlier in their life cycle, thus reducing risks of exfiltration of any confidential company information.

Internal Threat Intelligence

Enterprises are encouraged to set up their own threat intelligence group, which should focus on learning about exploits and the TTPs threat actors use. This group's role is critical in processing and understanding the data that resides on the network. The information the group gleans should be handed over to the security team so it can

4 Nart Villeneuve and David Sancho. (2012). "The 'Lurid' Downloader." Last accessed March 4, 2014, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_dissecting-lurid-apt.pdf.

5 David Sancho, Jessa dela Torre, Matsukawa Bakuei, Nart Villeneuve, and Robert McArdle. (2012). "IXESHE: An APT Campaign." Last accessed March 4, 2014, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_ixeshe.pdf.

6 Trend Micro Threat Research Team. (2012). "The Taidoor Campaign: An In-Depth Analysis." Last accessed March 4, 2014, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_the_taidoor_campaign.pdf.

7 Nart Villeneuve. (2011). "Trends in Targeted Attacks." Last accessed March 4, 2014, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_trends-in-targeted-attacks.pdf.

be incorporated into security systems. The group can also recommend how the enterprise can defend its network against threats. Trend Micro senior threat researcher, Jim Gogolinski, tackled how threat intelligence can thwart potential and ongoing targeted attack campaigns in his paper, "Suggestions to Help Companies with the Fight Against Targeted Attacks."[8]

External Threat Intelligence

External threat intelligence providers refer to third parties that offer threat intelligence deliverables such as reports on new campaigns and threats. They also provide feeds or data such as lists of malicious URLs and email headers, among others.

Trend Micro™ Deep Discovery can protect enterprises and large organizations against targeted attacks by detecting malicious content, communications, and behaviors that indicate attacker activity in a network.[9] It has custom sandbox simulation and advanced detection engines that classify and analyze submitted files. It also provides network traffic inspection, advanced threat detection, and real-time analysis and reporting, thus mitigating the risks targeted attacks pose before threat actors reach the data exfiltration stage.

Knowledgeable Human Analysts

Knowledgeable human analysts who process and make sense of logs and data collected from and transmitted over a network are an integral part of defending against targeted attacks. By making sense of threat intelligence, they can provide various defense strategies against any security threat that an enterprise may encounter. As such, combining threat intelligence, knowledgeable human analysts, and security solutions can help mitigate the risks threats such as targeted attacks pose.

8 Jim Gogolinski. (2013). "Suggestions to Help Companies with the Fight Against Targeted Attacks." Last accessed march 4, 2014, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_trends-in-targeted-attacks.pdf.

9 Trend Micro Incorporated. (2014). "Trend Micro Deep Discovery." Last accessed March 4, 2014, http://www.trendmicro.com/cloud-content/us/pdfs/business/datasheets/ds_deep-discovery.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