Operation ENDTRADE: Multi-Stage Backdoors that TICK

blog.trendmicro.com/trendlabs-security-intelligence/operation-endtrade-finding-multi-stage-backdoors-that-tick/

November 29, 2019

While we have been following cyberespionage group TICK (a.k.a. “BRONZE BUTLER” or “REDBALDKNIGHT”) since 2008, we noticed an unusual increase in malware development and deployments towards November 2018. We already know that the group uses previously deployed malware and modified tools for obfuscation, but we also found TICK developing new malware families capable of detection evasion for initial intrusion, as well as escalation of administrative privileges for subsequent attacks and data collection. We also found the group using legitimate email accounts and credentials for the delivery of the malware, zeroing in on industries with highly classified information: defense, aerospace, chemical, and satellite industries with head offices in Japan and subsidiaries in China. Given their targets, we have named this campaign “Operation ENDTRADE,” and identified some of the findings in our research *“Operation ENDTRADE: TICK’s Multi-Stage Backdoors for Attacking Industries and Stealing Classified Data”*.

This research paper was submitted and presented for the DeepINTEL Security Intelligence 2019 Conference on November 27, 2019 in Vienna, Austria.

Targeting and malware delivery

Figure 1. Operation ENDTRADE’s timeline

As part of their attacks in January 2019, TICK was conducting their research by compromising a Japanese economic research company and a public relations (PR) agency to steal email credentials and files as decoy documents. These email addresses were used for spear phishing, prompting potential victim organizations to open the attachments with malware payloads. Meanwhile, the documents were embedded with malware, and sent to individuals and companies knowledgeable in Japanese or Chinese, and interested in the Chinese economy. The emails had the following features:

- They were sent from legitimate email accounts
- They were written as legitimate reports and prompted the users to open the attachments
- They contained subject topics related to “salary rate increase” or “job market,” or with special interests in the economic affairs of China such as the US-China trade mandates

Figure 2. Spear phishing sample in fluent Japanese

Based on the language that was hardcoded in the samples we found, TICK appeared to be targeting Japanese organizations with subsidiaries in China to serve as footholds for intrusion: TICK hard-coded two code pages 932 and 936, referring to Japanese and Simplified Chinese characters respectively. Moreover, we found successful transfers of malicious executable files in the shared folder from a Chinese subsidiary with an infected desktop, and an employee in Japan that executed the said file.

Figure 3. Language code pages

While we found intrusions in a large number of companies in the abovementioned industries before May 2019, further analysis revealed that one of the main targets was the defense sector. We found TICK trying to steal military-related documents from the victim network during an extended assistance for incident response in the region. However, TICK seemed to shift their attention to the chemical industry by mid-May, which may indicate the group’s sponsor organization’s goal: To steal proprietary and classified information such as military data and advanced materials.

Malware Analysis

Our research lists some of the new and adjusted malware routines we found from Operation ENDTRADE, which we named based on their characteristic program database (PDB) strings. For a complete list and analyses of the trojans, downloaders, and modified tools, you may access the research brief here.

Figure 4. New downloaders and trojans

DATPER

While this backdoor routine has been associated with TICK's weapons arsenal, the sample we derived from this campaign had two adjusted mutex objects — *d0ftyzxcdrfdqwe* and **&Hjgfc49gna-2-tjb* — that retrieve information from the victim's machine. The latest variant also has a new set of parameters that allow it to evade anti-virus (AV) product pattern detections, implying the ease by which the group can change their routines to suit their goals.

Figure 5. DATPER's new mutex with separate parameters

down_new

This malware combines features of existing trojans in the malware family's development, based on the adjustments TICK made as we analyzed their test versions. It adds features (listed below) that can be found separately on previous iterations:

- Adds Autorun to the registry.
- Gets MAC address and volume information to send back to the C&C.
- Executes only during working hours (8:00AM-6:00PM, using *kernel32.GetLocalTime* API)
- Uses AES encryption and base64 encoding method to encrypt the call back message.
- Uses legitimate websites for the C&C server.
- Detects anti-virus products and processes.

Figure 6. Code showing down_new's command function

Table 1. down_new command list

As we studied its processes to compare with the others, the call back information stood out: The HTTP post header is hard-coded in the sample, getting the infected machine's specific information to single out the identity of the users. As a cyber-espionage group with specific goals based on their sponsoring organization's objectives, TICK only goes after specific targets and only uses other non-targeted individuals and enterprises as footholds to meet their purposes.

Figure 7. down_new collects home phone data and URL path

Avenger

Our analysis found that Avenger has a number of variants and versions depending on their targets. For example, some variants have autorun functions while others execute a sleep mode upon system infection. We found that the downloader has three stages:

1. The first stage collects volume information, AV product, and OS bits version from the host, and sends it to the command and control (C&C) server to ensure that the host is the intended target.

Figure 8. First stage: Information collection

2. It then checks if the host matches their C&C server reference. Avenger collects the victim’s detailed information from the system by browsing the folders, files, and domain information.

Figure 9. Second stage: Collected information is written into a .txt file

3. If the host doesn’t exist, Avenger will download an image with an embedded malware hidden via steganography and extract a backdoor.

Figure 10. Third stage: Sending the encrypted file to the C&C

While steganography is always used as part of TICK’s malware techniques, we found that the group used a more sophisticated steganography technique in this campaign.

Figure 11. Backdoor found in the steganography image

Figure 12. Upgraded steganography technique

We found a newer version of Avenger with a clearer code structure and internal IP testing URL (aptly named Avenger2 in the PDB strings), though the rest of the components had minimal differences with the previous version.

Figure 13. Avenger2 with internal URL

Casper

Casper is a modified version of the Cobalt Strike backdoor, showing the team server SHA1 hash if the controller connects to the C&C. If accessed by the client, Cobalt Strike confirms with the user if they recognize and match the SHA1 hash of a specific team server’s SSL certificate.

Figure 14. Casper C&C with Cobalt Strike’s server fingerprint

The backdoor is usually hidden in the steganography photo and uses several techniques and tools to bypass AV detection. One technique involves launching itself with a legitimate Windows application with Dynamic Link Library (DLL) side loading techniques. Another involves injecting the backdoor’s shellcode into *svchost.exe*.

Figure 15. Shellcode injected to svchost.exe

Publicly available RATs and modified tools

Included in all the malware routines, we also found TICK using publicly available remote access trojans (RATs) and ope n source tools, and either modified or imported the techniques into their malware. For instance, they cloned Lilith RAT from GitHub, studied and implemented its features into their customized backdoor under continued development. The list of modified tools the group used include Mimikatz, RAR compression tool, port mapping tool, and screen capture.

Figure 16. Modified screen capture tool

Figure 17. Modified Mimikatz

Conclusion

TICK is an organized and persistent cyber espionage group specialized in targeting high-value individuals and organizations, with the skills and resources needed to coordinate sophisticated attacks.

This operation not only highlights the need for stronger monitoring systems foremost in countries' critical infrastructures and multinational enterprises, but also firmer operational chains of command and redundant security policies established. Persistent criminal groups will continue to target enterprises, and will look for security gaps to exploit to gain unauthorized entry. Organizations with foreign subsidiaries can make it difficult to take control and implement security procedures and policies, making monitoring, isolating, investigating, incident response, and recovery more difficult. To top it all, employees' security awareness and consciousness will remain a significant part of making sure the security measures in place are maintained for regular operations.

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 TICK's attacks even without any engine or pattern update. Trend Micro™ Deep Security™ provides virtual patching that protects endpoints from threats that abuses unpatched vulnerabilities.

Trend Micro's suite of security solutions is powered by XGen™ security, which features high-fidelity machine learning to secure the gateway and endpoint data and applications. XGen™ protects against today's purpose-built threats that bypass traditional controls, exploit known, unknown, or undisclosed vulnerabilities, and either steal or encrypt personally-identifiable data.

For the full technical analyses of all the malware, techniques, tools, MITRE ATT&CK techniques and indicators of compromise (IoCs) we found in this campaign, download the research brief, *"Operation ENDTRADE: TICK's Multi-Stage Backdoors for Attacking Industries and Stealing Classified Data"*.