MegaCortex Ransomware Spotted Attacking Enterprise Networks

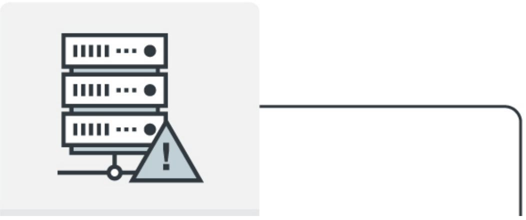
trendmicro.com/vinfo/pl/security/news/cybercrime-and-digital-threats/megacortex-ransomware-spotted-attacking-enterprise-networks

A new ransomware called MegaCortex (Trend Micro detects this as RANSOM.WIN32.CORTEX.SM) has been reportedly deployed against large corporate networks and workstations in the United States, Canada and parts of Europe. Cybersecurity firm Sophos first reported a sharp spike in MegaCortex activity last Friday noting that 47 attacks were stopped within 48 hours, which is two-thirds of all known incidents involving this ransomware. This recent surge isn't the earliest encounter with the ransomware — the first known sample was uploaded on January in the public sharing site VirusTotal.

How MegaCortex works

At least one victim reported that the attack originated from compromised domain controllers inside the enterprise network, but it isn't clear how the ransomware distributors gained access to the networks.

After gaining access to the domain controller, the attackers configured it to distribute a batch file, a renamed PsExec, and *winnit.exe*, which is one of the main executables of the malware, to the rest of the computers on the network. After this step, they run the batch file remotely. This file will terminate Windows processes as well as stop and disable services that will interfere with the ransomware's routines.



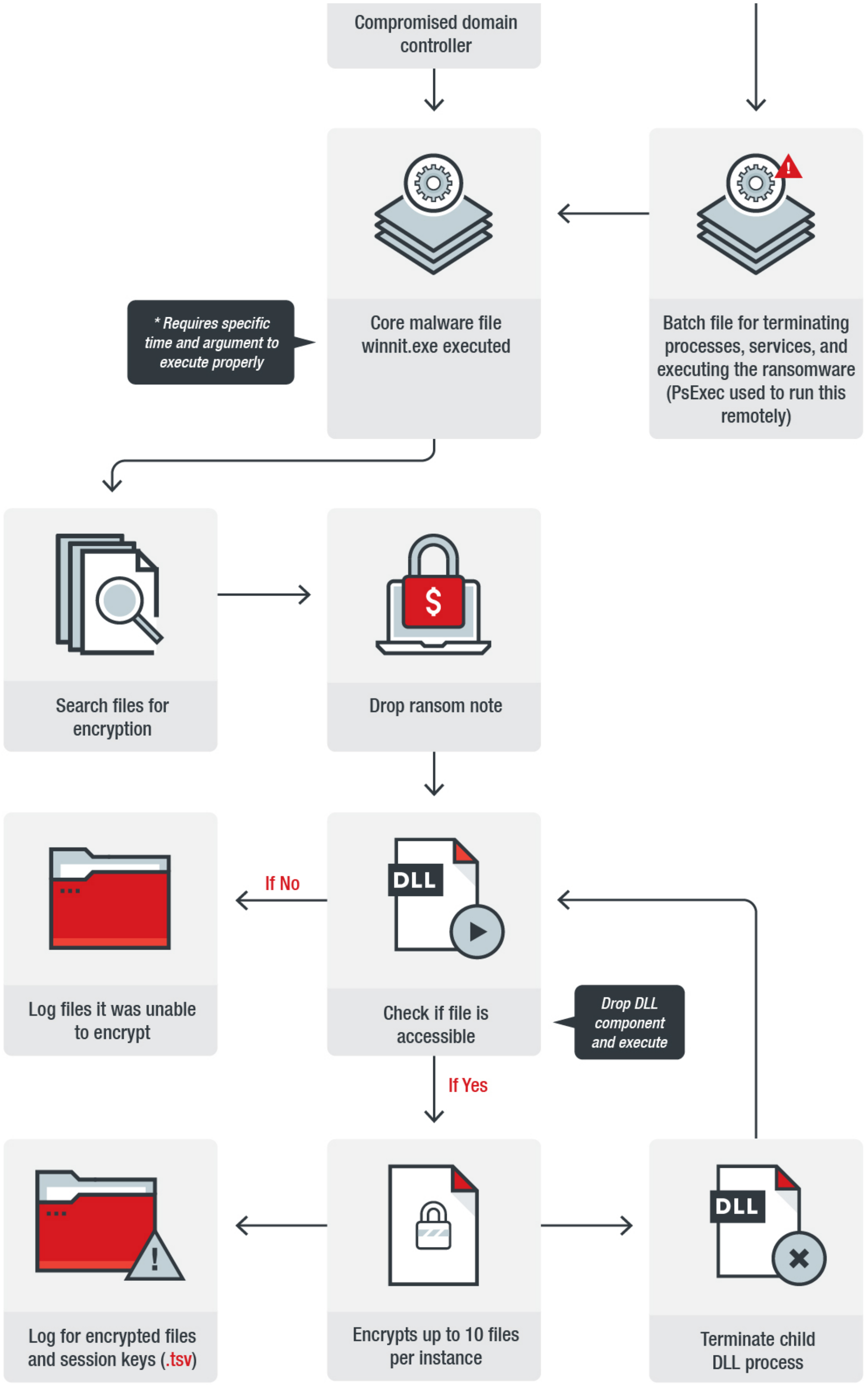

Compromised domain controller
Core malware file winnit.exe executed
Batch file for terminating processes, services, and executing the ransomware (PsExec used to run this remotely)
* Requires specific time and argument to execute properly
Search files for encryption
Drop ransom note
$
Log files it was unable to encrypt
If No
DLL
Check if file is accessible
Drop DLL component and execute
If Yes
Log for encrypted files and session keys (.tsv)
Encrypts up to 10 files per instance
DLL
Terminate child DLL process

Figure 1. Infection chain of MegaCortex

The batch file then executes *winnit.exe*, the core malware file, during a specific time frame and with specific Base64 argument. If executed properly, the malware will search files for encryption and drop a ransom note. It will also extract a randomly-named DLL and execute it with *rundll32.exe*. This DLL is the component that will encrypt the computer's files. It will first check if the file is accessible. If not, it will simply log the files. If it is accessible, the file will be encrypted, the child DLL process will be terminated after a set number of file encryption attempts, and the cycle will start again.

When encrypting the victim's files, the ransomware will append the extension *.aes128ctr*. According to Sophos, the ransomware will also generate a file with a *.tsv* extension and drop it in the hard drive. The MegaCortex actors' ransom note instructs the users to submit this file to them because it contains encrypted session keys needed for decryption. The ransom note itself is a *.txt* file that doesn't ask for the usual cryptocurrency payment, instead it demands that victims buy the actor's software.

In addition to the main payload, the malware also drops secondary components that security researchers have identified as the Rietspoof malware, a delivery system used to drop multiple payloads onto a device.

Defending against ransomware

Users and businesses are recommended to adopt best practices to defend against ransomware: Regularly back up files, keep the system and applications updated, enforce the principle of least privilege, and implement defense in depth — arraying security at each layer of a company's online perimeters, from gateways, networks, endpoints, and servers.

Trend Micro Ransomware Solutions

Enterprises can benefit from a multilayered approach to best mitigate the risks brought by ransomware. At the endpoint level, Trend Micro Smart Protection Suites deliver several capabilities like high-fidelity machine learning, behavior monitoring and application control, and vulnerability shielding that minimize the impact of this threat. Trend Micro Deep Discovery Inspector detects and blocks ransomware on networks, while Trend Micro™ Deep Security™ stops ransomware from reaching enterprise servers — whether physical, virtual, or in the cloud. Trend Micro™ Deep Security™, Vulnerability Protection, and TippingPoint provide virtual patching that protects endpoints from threats that exploit unpatched vulnerabilities to deliver ransomware.

Email and web gateway solutions such as Trend Micro™ Deep Discovery™ Email Inspector and InterScan™ Web Security prevent ransomware from ever reaching end users. Trend Micro's Cloud App Security (CAS) can help enhance the security of Office 365 apps and other cloud services by using cutting-edge sandbox malware analysis for ransomware and other advanced threats.

These solutions are powered by Trend Micro XGen™ security, which provides a cross-generational blend of threat defense techniques against a full range of threats for data centers, cloud environments, networks, and endpoints. Smart, optimized, and connected, XGen™ powers Trend Micro's suite of security solutions: Hybrid Cloud Security, User Protection, and Network Defense.

Updated as of May 15, 2019 9:30AM: Added image and information about MegaCortex infection chain
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.

Opublikowany w Cybercrime & Digital Threats, Ransomware