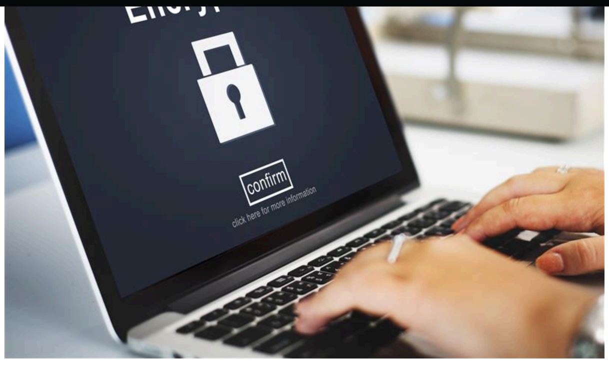
MegaCortex Ransomware Spotted Attacking Enterprise Networks

May 07, 2019

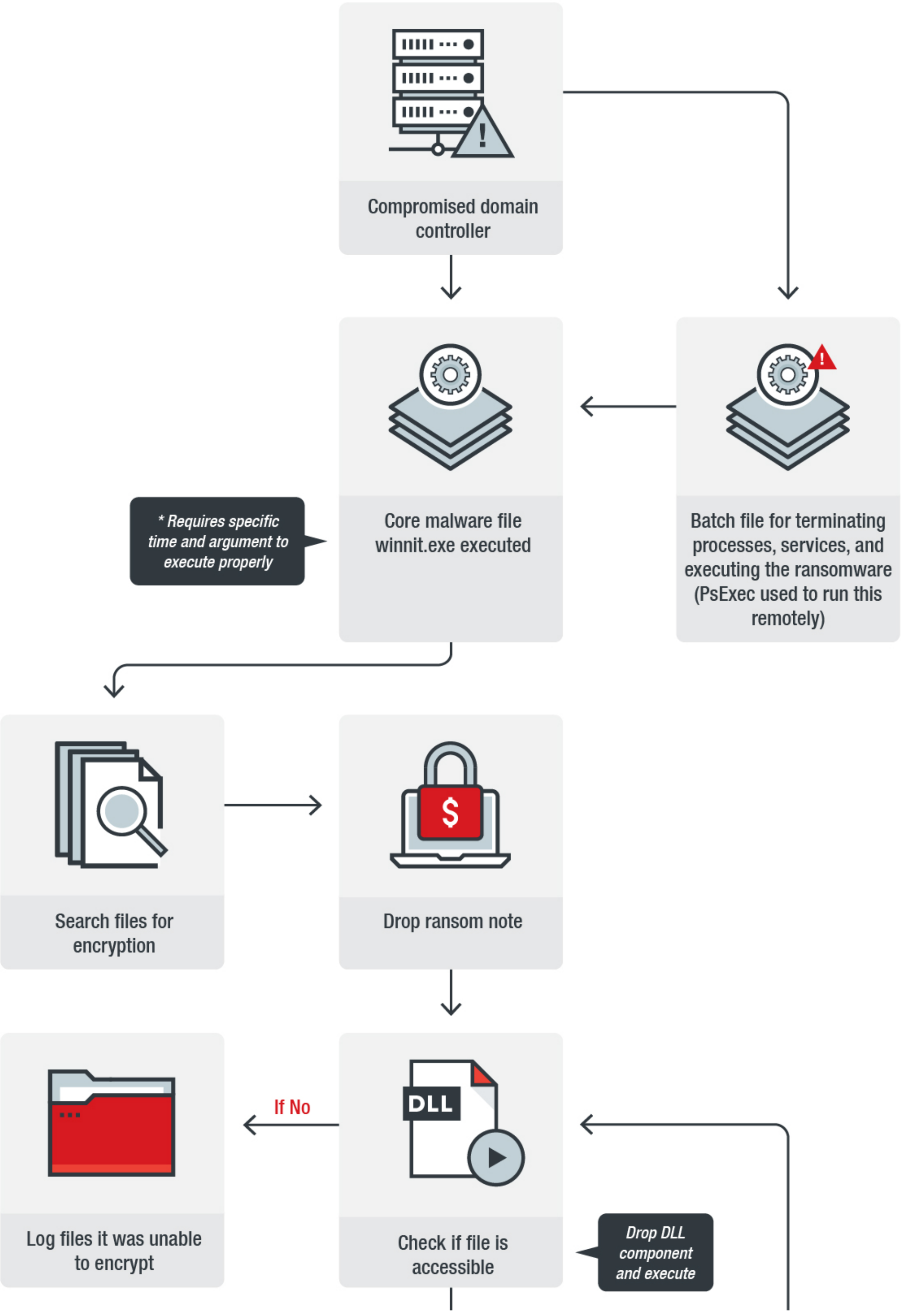


RANSOM.WIN32.CORTEX.SM) has been reportedly deployed against large corporate networks and workstations in the United States, Canada and parts of Europe. Cybersecurity firm Sophos first reported a sharp spike in MegaCortex activity last Friday noting that 47 attacks were stopped within 48 hours, which 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
Check if file is accessible
Drop DLL component and execute
DLL

Ransomware Spotlight: INC
Phobos Emerges as a Formidable Threat in Q1 2024, LockBit Stays in the Top Spot: Ransomware in Q1 2024
Ransomware Spotlight: LockBit
Rise in Active RaaS Groups Parallel Growing Victim Counts: Ransomware in 2H 2023
Calibrating Expansion: 2023 Annual Cybersecurity Report

Recent Posts

Cellular IoT Vulnerabilities: Another Door to Cellular Networks
Ransomware Spotlight: INC
The Realities of Quantum Machine Learning
Unchaining Blockchain Security Part 3: Exploring the Threats Associated with Private Blockchain Adoption
Generative AI in Elections: Beyond Political Disruption

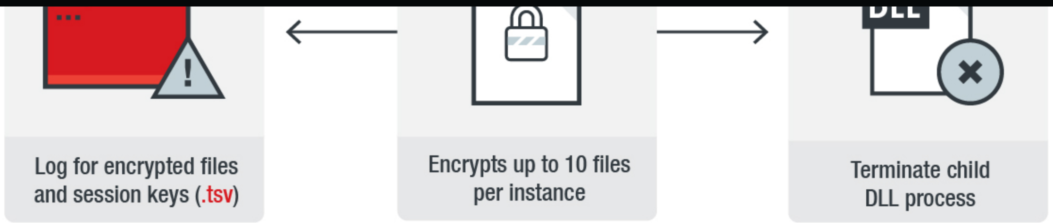

Log for encrypted files and session keys (.tsv)
Encrypts up to 10 files per instance
DLL
Terminate child DLL process

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 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

Posted in Cybercrime & Digital Threats, Ransomware

We Recommend

Internet of Things

Cellular IoT Vulnerabilities: Another Door to Cellular Networks

UNWIRED: Understanding the Unforeseen Risks in Evolving Communication Channels

MQTT and M2M: Do You Know Who Owns Your Machine's Data?

Virtualization & Cloud

Today's Cloud and Container Misconfigurations Are Tomorrow's Critical Vulnerabilities

Uncover Cloud Attacks with Trend Vision One and CloudTrail

Kong API Gateway Misconfigurations: An API Gateway Security Case Study

Ransomware

Ransomware Spotlight: INC

Phobos Emerges as a Formidable Threat in Q1 2024, LockBit Stays in the Top Spot: Ransomware in Q1 2024

Ransomware Spotlight: LockBit

Security Technology

The Realities of Quantum Machine Learning

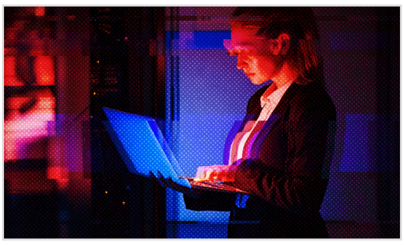
API Security Exposed: The Role of API Vulnerabilities in Real-World Data Breaches

Post-Quantum Cryptography: Migrating to Quantum Resistant Cryptography

Critical Scalability: Trend Micro Security Predictions for 2024

View the 2024 Trend Micro Security Predictions

Calibrating Expansion: 2023 Annual Cybersecurity Report



View the report

Resources

Blog

Newsroom

Threat Reports

Find a Partner

Support

Business Support Portal

Contact Us

Downloads

Free Trials

About Trend

About Us

Careers

Locations

Upcoming Events

Trust Center

Country Headquarters

Trend Micro - Hong Kong (HK)

903-905 9/F
Shui On Centre,
6-8 Harbour
Road Wanchai,
Hong Kong

Phone: +852-2214-3200