Carbanak threat details and protection using Trend Micro products

Updated: 6 Nov 2019 **Product/Version:** Deep Discovery Advisor 3.0 , **Platform:** Windows 2000 Advanced Server,

Rating:
1 found this helpful

Category:
Remove a Malware / Virus

Solution Id:
1107858

SUMMARY

Earlier this week Trend Micro received reports of a targeted attack that specifically affected banks and enabled attackers to steal large sums of money from affected companies by infiltrating the networks and modifying bank records.

This highlights a kind of threat that the banking industry faces differ, one that might not directly affect the end-users as with the case with phishing and online banking malware, but is equally or just as critical. Banks are networks that hold very critical financial data, which makes them perfect targets for cyber attacks.

According to reports, the attackers were able to infiltrate 100 banks located in various countries, including Russia, USA, Germany, China, and Ukraine. Here are the high-level details on how the infiltration was executed:

- **Spear phishing emails** were sent to the banks' employees, containing either an **exploit** (CVE-2012-0158, CVE-2013-3906, CVE- 2014-1761) or a **malicious CPL file**.
- Both the exploit and the malicious CPL file drop the Carbanak malware into the system. Carbanak **is a backdoor designed to execute various commands** including logging keystrokes, taking screenshots, and checking for specific banking applications such as fund transfer software.
- The attackers used Carbanak to **move laterally within the network** through remote administration tools to reach target systems, which are those that involve processing bank accounts. Once target systems are reached, the attackers record videos of the affected user's operation to be familiar with the victim's workflow. The attackers then used this information and access to manipulate bank records and transfer funds into their accounts without being detected.

This attack is notable for its usage of techniques that aimed to mimic normal activities within the network in order to evade detection. It raises the importance of having a security strategy that is designed to see through these techniques and detect malicious activities.

DETAILS

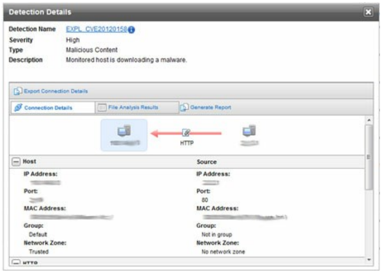
Custom Defense Solutions

Trend Micro Custom Defense employs a comprehensive 360-degree detection to minimize the opportunities for a targeted attack through its family of security solutions.

Trend Micro Deep Discovery provides the network-wide visibility and intelligence that is the cornerstone of the Custom Defense solution against so-called APTs (advanced persistent threats) and targeted attacks such as this one.

For the Carbanak attack scenario, Deep Discovery could detect the attack at several different points in the sequence of events:

- Trend Micro Deep Discovery Email Inspector is able to detect the spear-phishing emails sent by attackers to the banks' employees as the initial step to breach traditional security defenses, establish a foothold, and commence a targeted attack. Deep Discovery Email Inspector has email inspection capabilities that discover malicious content, attachments, and URL links that pass unnoticed through standard email secu



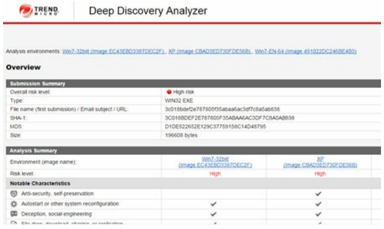
Detection Details

Detection Name: EXPL_CVE20120158
Severity: High
Type: Malicious Content
Description: Monitored host is downloading a malware.

Host	Source
IP Address: [redacted]	IP Address: [redacted]
Port: [redacted]	Port: 80
MAC Address: [redacted]	MAC Address: [redacted]
Group: Default	Group: Not in group
Network Zone: Trusted	Network Zone: No network zone

HTTP

- Trend Micro Deep Discovery Analyzer is able to detect even previously unknown threats by analyzing a broad range of file types, sizes, and sources using customizable sandbox environments that attackers design and build to match organization's desktop and device platforms. It enhances the malware detection capabilities of all existing security investments by giving the ability to share detected and analyzed threat insight, enabling security infrastructure to prevent malicious communication, websites, applications, malware and attacker behavior from spreading.



TREND MICRO | Deep Discovery Analyzer

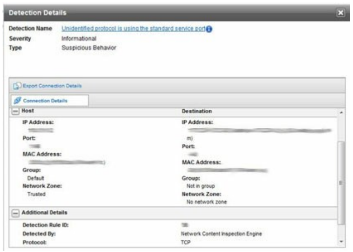
Analysis environments: Win7-32bit (Image EC43EBD3387DEC2F) , XP (Image CBAD3ED730FDE56B) , Win7-EN-64 (Image 491022DC246BE4B3)

Overview

Submission Summary	
Overall risk level:	● High risk
Type:	WIN32 EXE
File name (first submission) / Email subject / URL:	3c018bdef2e787805f35abaa6ac3df7c8a5ab838
SHA-1:	3C018BDEF2E787805F35ABAA6AC3DF7C8A5AB838
MD5:	D1DE522652E129C37759158C14D48795
Size:	196608 bytes

Analysis Summary		
Environment (image name):	Win7-32bit (Image EC43EBD3387DEC2F)	XP (Image CBAD3ED730FDE56B)
Risk level:	High	High
Notable Characteristics		
Anti-security, self-preservation		✓
Autostart or other system reconfiguration	✓	✓
Deception, social engineering	✓	✓
File drop, download, sharing, or replication	✓	✓

- Trend Micro Deep Discovery Inspector is able to identify suspicious activities anywhere on network, such as those executed by Carbanak in moving laterally through the network and connecting to its command and control. Deep Discovery Inspector is also able to proactively detect the traffic triggered by the remote administration tool used by attackers: Deep Discovery Inspector is capable of monitoring traffic across all ports and more than 80 protocols and applications to detect threats that are purposely built to evade traditional security defenses. It also features Trend Micro Advanced Threat Scan Engine that is able to detect the malicious email attachments with embedded exploit code through its forward-looking heuristic rules.



Detection Details

Detection Name: Unidentified protocol is using the standard service port
Severity: Informational
Type: Suspicious Behavior

Host	Destination
IP Address: [redacted]	IP Address: [redacted] m)
Port: [redacted]	Port: [redacted]
MAC Address: [redacted]	MAC Address: [redacted]
Group: Default	Group: Not in group
Network Zone: Trusted	Network Zone: No network zone

Additional Details	
Detection Rule ID:	[redacted]
Detected By:	Network Content Inspection Engine
Protocol:	TCP

Once detected, Deep Discovery can provide the organization with both local intelligence and global threat intelligence from the Trend Micro Smart Protection Network to identify and assess the risk of the malware, communications or activities found.

Finally, Deep Discovery provides automated security signature updates and alert notifications to the organizations's other security products to enable a full Custom Defense that stops the attack from progressing further. Examples include:

- Providing IOC (Indicators of Compromise) information including C&C blacklists to both Trend Micro and third party security products
- SIEM alerting and full IOC sharing
- Optionally invoking Trend Micro Network VirusWall Enforcer to isolate endpoints known to be infected

Endpoint Protection

Properly-configured endpoint solutions can ensure the prevention of Carbanak from coming into the machine or network.

- Components of OfficeScan Corporate Edition (OSCE) such as SmartScan, Web Reputation Service, Behavior Monitoring, and Smart Feedback offer the best protection against Carbanak by detecting the malicious files.

- Worry-Free Business Security/Services (WFBS/WFBS-SVC) is also equipped with technologies to detect and remove Carbanak in the machine or network

Mail Scanning Solution

Email played a big part in the delivery of Carbanak, making it an important vector to protect from attackers.

- Trend Micro Hosted Email Security offers technologies such as the connection-level and content-based reputation filtering, designed best to block threats that arrive via email.
- Trend Micro InterScan Messaging Security Virtual Appliance leverages the Trend Micro Advanced Threat Scan Engine in order to detect document exploits such as the ones used in this attack.

FEEDBACK

Did this article help you? Yes No