VISA SECURITY ALERT

March 2015

CARBANAK (ANUNAK) ADVANCED PERSISTENT THREAT

Distribution: Merchants, Issuers, Acquirers, Processors

Audience: IT, Information Security, Risk Management

Summary

In February 2015, researchers from Kaspersky Labs discovered an Advanced Persistent Threat (APT) style attack on financial institutions (FIs) and retailers, primarily located in Ukraine, Russian, and Eastern Europe. Since at least 2013, a cybercriminal group has used malware, identified as Carbanak, with a sophisticated cybercrime campaign to commit financial fraud. According to Kaspersky Labs, more than 100 financial institutions (FI) and retailers have been affected. Reports indicate that the impacted institutions have suffered estimated losses of US$1 billion thus far. Attacks conducted as a part of this threat activity are reportedly still ongoing.

Description and Impact

Kaspersky Labs has reported that over 100 FIs and retailers in over 30 countries were targeted with spear phishing emails that are designed to appear to be legitimate banking communications with Microsoft Word 97-2003 (.doc) and Control Panel Applet (.cpl) files attached. Once the email attachments were opened by employees, the attachments launched an exploit backdoor named Carbanak.

Once the Carbanak backdoor is launched, the malware allows attackers remote access a target's network and perform manual reconnaissance to locate critical systems and infrastructure. The primary targets of the attackers were Automated Teller Machines (ATMs), money processing services, and financial accounts. The attackers were able to modify Oracle databases to change account balances, create bank accounts to wire money out of the FIs, and dispense cash from various ATMs where the attackers would be ready to retrieve the cash from identified machines.

In some cases, video recordings of bank teller operations were made, keystrokes were captured, and sent back to the attackers to learn and mimic legitimate transactions. Attackers would inflate account balances and withdraw the added amount to avoid suspicious and detection. For example, an account with $1,000 would be inflated to $10,000 and the attacker would transfer the $9,000 difference so that the account holder would not suspect any changes to the account.

Kaspersky Labs estimates that the financial losses per bank range from $2.5 million to $10 million, and that total losses may be as high as US $1 billion. The group responsible for the attack is still active and it is recommended that all FIs and retailers scan their networks for the presence of Carbanak. If detected, please contact law enforcement immediately and activate security incident procedures.

Detection and Mitigation

It is recommended that FIs and retailers scan their network for the following:

- Paexec file
- Files with .bin extension (located in \All users\%AppData%\Mozilla\ or c:\ProgramData\Mozilla\)
- Svchost.exe file (located in Windows\System32\com\catalogue\)
- Operating system (Windows) running services ending in "sys"

Additionally, Visa suggests the follow measures to reduce the risk of exposure to Carbanak:

- Educate employees about phishing scams and avoiding opening emails with attachments
- Maintain updates for all software and patches (address zero day vulnerabilities)
- Turn on heuristics (behavioral analysis) on anti-malware to search for suspicious behavior

External Links:

Kaspersky Labs: Carbanak APT: The Great Bank Robbery

Group-IB/Fox-IT: Anunak: APT Against Financial Institutions

To report a data breach, contact Visa Fraud Control:

- Asia Pacific Region, Central Europe/Middle East/Africa Region: VIFraudControl@visa.com
- U.S. and Canada: USFraudControl@visa.com

For more information, please contact Visa Risk Management: cisp@visa.com