COLORTOKENS

THREAT RESEARCH

Jointworm Group Sets Eyes on Financial Services Organizations

What is Jointworm?

Jointworm, a sophisticated attack group, has been involved in campaigns targeting companies in the financial sector since the start of the year 2020, and appears to have gathered steam over the last couple of months with a clear upward trend of ransomware detections on the systems of financial organizations since Sep 2020.

Through these attacks, Jointworm is trying to steal financial information from targeted companies, including email credentials, customer credit card information, cookies and session information, software licenses etc. These campaigns seem to be still ongoing, hence financial organizations need to be aware of such professional threat groups.

Who has been targeted?

In its most recent campaign, Jointworm primarily targeted financial services companies in Cyprus, Ukraine, the U.S., and Czech Republic, including those that operate within the stock exchange markets, and some high-tech companies that develop technologies for financial organizations (also known as FinTech companies). A media company was also targeted in this campaign.

During the campaign, the threat group spent a significant amount of time on the networks of some of its victims, maintaining its presence on the network of one financial sector victim for 184 days and on another victim's network for 123 days.

Tactics and techniques used by Jointworm

From the insights derived from Jointworm's recent campaign that targeted several financial organizations' networks, we observed the following techniques being used by attackers:

1. Initial Access: The group uses email as its initial attack vector and showcases generic, financially related lures and attachment names in the emails. The malicious email links to an archive file on a trusted cloud provider that contains an LNK file masquerading as a document or image with embedded JavaScript file to install a backdoor.

2. Execution of Commands: Arbitrary Commands via MSXSL and CMSTP are executed on infected systems to install backdoors. After the installation of the backdoor, powershell commands are executed to download additional tools and malware through the abuse of legitimate admin tools on infected machines.

3. Privilege Escalation: The string "cpassword" is a command string found in XML files linked to group policies. Passwords extracted from these files are easily decrypted and abused by attackers to perform privilege escalation to a network admin's account.

4. Credential Access: A loader file (24067.ocx) is executed, presumably to load a Metasploit module for extended remote access. Further, Mimikatz is deployed to dump credentials across multiple machines within victim organizations.

5. Lateral Movement: Group policy files are accessed and the encrypted passwords from the XML file are decrypted to move laterally across the network.

6. Collection of General Information: WMIC is used across several compromised machines to collect general information, such as local storage information, BIOS Serial Number, Mac Address etc.

7. Command and Control: A connection to attacker-controlled infrastructure is established by deploying Python reverse shell across multiple machines by copying legitimate Python interpreter executable (rev.exe) to execute the Python file.

8. Data Exfiltration: Upon completion of the above tactics, attackers start exfiltrating data using C2 and non C2 channels (Internet accessible locations).

ColorTokens Security Solution for Preventing Ransomware Attacks

ColorTokens solutions provide 100% protection from most sophisticated ransomware attacks targeting financial sector organizations:

Xprotect's protection levels have been enhanced by updating security profiles to block execution of unwanted scripts/processes such as JScript/Python/Arbitrary commands and others.

Advanced Rule rings are implemented to stop misuse of processes such as 'cmd.exe spawning PowerShell.exe'.

Xshield ensures the impact radius is minimized through enforced policies.

Our threat intelligence is consistently updated with identified IOCs of hash, IP and domains, providing real-time protection to customers from any such known attacks.

Our experts offering Breach Protection Services monitor and detect attack patterns and suspicious behaviours around-the-clock. For instance, usage of suspicious commands, and suspicious behaviour on execution of authorized and whitelisted processes etc.

Indicators of Compromise (IoCs)

Here are some sample IoCs

1820244e54dbb87ea21f6f1df15c3f255bfe3dd36db41fbf2f2e1f742a515063
1be727ebce44e5c669b2b08ad06e9d99c02490f8bb7f59dda81050947d99b77a
30970d1144705a7a6cc874db67094fff19a0ed99a559f21e58a858fe5c1d01f8
4c355d1e1a2a10135aa2e2848790355bfbab2d64eb5dd95d7278cd8c0ffbf470
a53e5b8da9a397fbf3623969333fb7c58e7690e8dbd0f485c1d7861e3e07fe37
fd50f667337214e27256a0a8053e321d54c61466dce61805bdf51ca47e89e567
aa386dc2f66e2527766f50f5dd75f023550725ea8afc68593a596c41620265bc

References

https://symantec.broadcom.com/hubfs/SED-Threats-Financial-Sector.pdf