Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

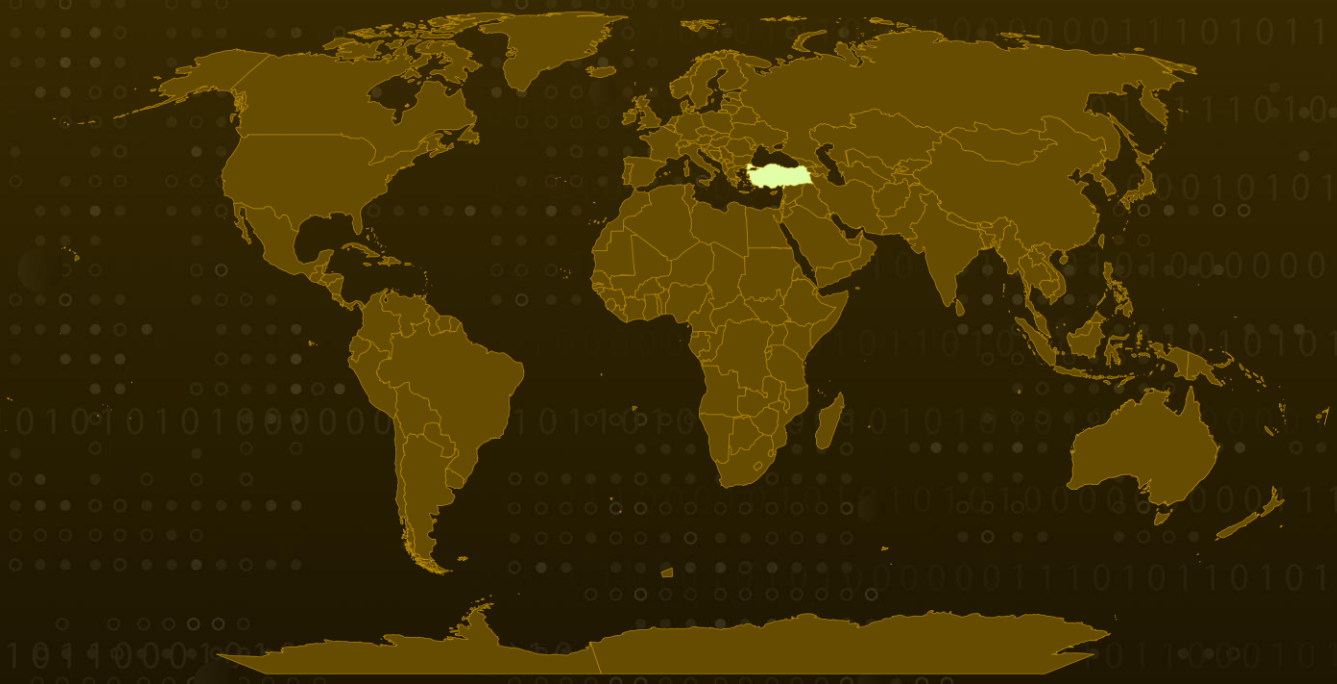
ShadowRoot Ransomware a Menace to Turkish Enterprises

Date of Publication	Admiralty Code	TA Number
July 16, 2024	A1	TA2024274

Summary

Malware: ShadowRoot Ransomware
Attack Region: Turkey
Targeted Industries: Businesses, Healthcare, and E-Commerce
Attack: ShadowRoot Ransomware is an advanced malware threat targeting businesses in Turkey. The attack begins with an email containing a PDF attachment embedded with a URL link. This link guides recipients to download a malicious executable file from a compromised GitHub account.

Attack Regions



Attack Details

#1 ShadowRoot Ransomware is a sophisticated malware that targets businesses in Turkey. The attack typically begins when victims receive an email containing a PDF embedded with a URL link. This link leads them to download a malicious executable file from a compromised GitHub account.

#2 Once downloaded, this 32-bit Borland Delphi binary executes and deposits additional payloads, including `RootDesign.exe`, into a designated directory on the victim's computer.

#3 To evade detection by security software, the dropped payload employs .NET obfuscation techniques, making it challenging for standard security protocols to identify and halt malicious activities. The ransomware then creates specific mutexes, and synchronization objects, to efficiently manage its processes.

#4 Following this, it initiates the encryption process, targeting critical system and office files. These encrypted files are appended with a ".ShadowRoot" extension. The encryption process is meticulous, logging its activities and spawning multiple recursive threads that significantly consume system memory. Upon encrypting the files, the ransomware deposits a ransom note written in Turkish named "readme.txt" on the desktop.

#5 In addition to encrypting files, ShadowRoot Ransomware also exfiltrates data. It connects to a Russian SMTP mail server and transmits the stolen data to the attackers' email accounts, ensuring the information is exfiltrated without immediate detection. This amalgamation of sophisticated techniques renders ShadowRoot Ransomware a formidable threat to businesses, severely disrupting operations and compromising data security and financial stability.

Recommendations

Email Security: Implement advanced email filtering and phishing detection systems to block malicious attachments and URLs. Educate employees about phishing tactics and encourage cautious handling of email attachments and links.

Implement Network Segmentation: Segment your network to isolate critical systems and sensitive data from general user access and potential malware spread. Use intrusion detection and prevention systems (IDPS) to monitor and analyze network traffic for abnormal behavior.

Data Backups: Implement frequent backups for all assets to ensure their complete safety. Implement the 3-2-1-1 backup structure and use specialized tools to provide backup resilience and accessibility.

Content Filtering and Application Control: Enforce application control to prevent unauthorized app installations and executions, reducing the risk of downloading and running malicious files. This integrated strategy safeguards against downloadable threats by proactively blocking access to harmful content and preventing the execution of malicious code.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0005** Defense Evasion
TA0007 Discovery	**TA0009** Collection	**TA0011** Command and Control	**TA0010** Exfiltration
TA0040 Impact	**T1204** User Execution	**T1204.002** Malicious File	**T1082** System Information Discovery
T1562 Impair Defenses	**T1562.001** Disable or Modify Tools	**T1140** Deobfuscate/Decode Files or Information	**T1083** File and Directory Discovery
T1071 Application Layer Protocol	**T1486** Data Encrypted for Impact	**T1041** Exfiltration Over C2 Channel	**T1566** Phishing
T1598.003 Spearphishing Link	**T1059** Command and Scripting Interpreter	**T1059.001** PowerShell	**T1027** Obfuscated Files or Information
T1005 Data from Local System	**T1055** Process Injection		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	cd8fbf0dcdd429c06c80b124caf574334504e99a, 1c9629aeb0e6dbe48f9965d87c64a7b8750bbf93
URL	hxxps[:]//raw[.]githubusercontent[.]com/kurumsaltahsilat/detayfatura/main/PDF[.]FaturaDetay_202407[.]exe
Email	Kurumsal[.]tasilat[@]internet[.]ru, ran_master_som[@]proton[.]me, lasmuruk[@]mailfence[.]com

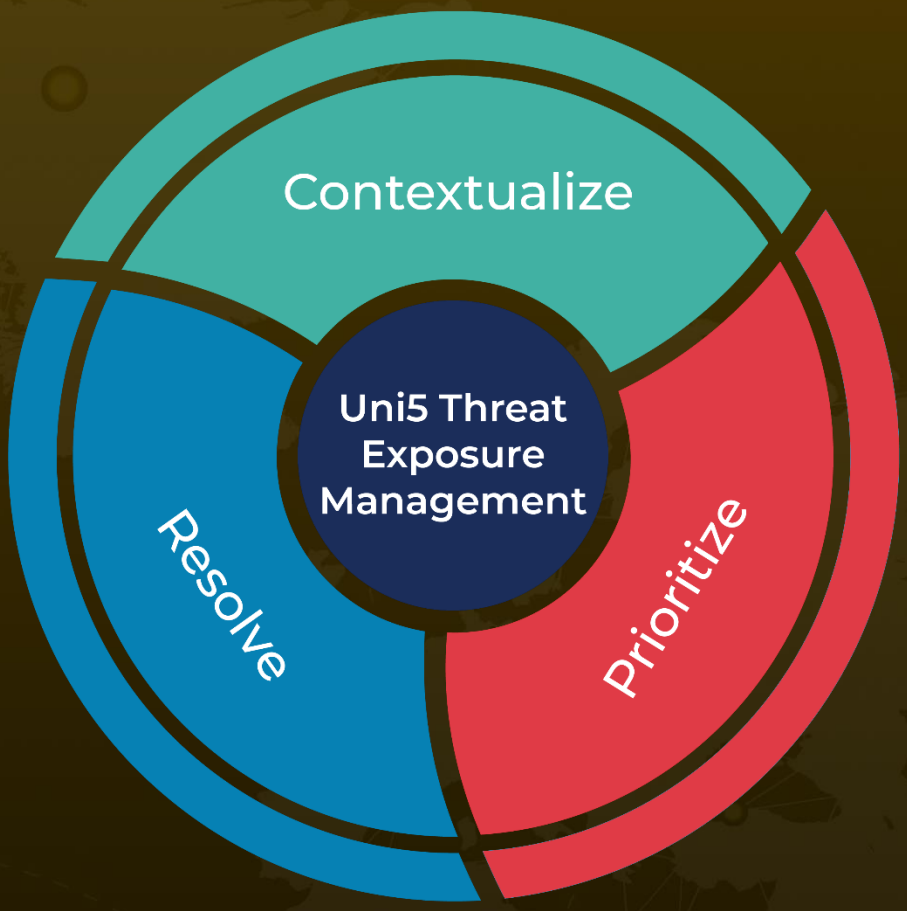
References

https://www.forcepoint.com/blog/x-labs/shadowroot-ransomware-targeting-turkish-businesses

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

July 16, 2024 • 7:00 AM

More at www.hivepro.com