Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

The Unrelenting Nature of TOITOIN Malware

Date of Publication	Admiralty Code	TA Number
July 11, 2023	A1	TA2023294

Summary

First appeared: May 2023
Malware: TOITOIN Trojan
Attack Region: Latin American (LATAM) region
Targeted Industries: Businesses, Banking
Affected platforms: Amazon EC2 instances
Attack: The TOITOIN malware campaign, targeting businesses in the LATAM region, employs sophisticated techniques and multi-stage infection chains with numerous malware samples disguised as compressed ZIP archives hosted on Amazon EC2.

Attack Regions

Attack Details

#1 The TOITOIN malware campaign focuses on businesses in the LATAM region, employing advanced techniques and multi-stage infection chains. In May 2023, several malware samples disguised as compressed ZIP archives were discovered and hosted on Amazon EC2. The TOITOIN campaign follows a meticulously crafted sequence, starting with a phishing email to compromise the target.

#2 Unknowingly to the user, this sets off a series of events that result in the covert download of a malicious ZIP archive onto their system and the gradual breach of their defenses. By leveraging the capabilities of Amazon's cloud infrastructure, the attackers have effectively evaded detection mechanisms based on domains, consistently maintaining an advantageous position.

#3 The downloader module in the zip archive commences a complex String Decryption process. Subsequent stages of the download maneuver cleverly bypass sandboxes by employing system reboots and establishing persistence through LNK files. The malware also checks system privileges and activates the COM Elevation Moniker to the BypassUAC module. The culmination unveils a novel Trojan known as TOITOIN, which utilizes an exclusive XOR decryption method to unravel its configuration file.

#4 Furthermore, the TOITOIN Trojan connects with the Command and Control (C&C) server, which gets the Windows version by querying the ProductName registry key value, as well as the environment variable and the path to the Program Files directory. The encrypted data is subsequently delivered to the C&C server using curl via a POST request.

Recommendations

Enhance email security measures to effectively detect and prevent phishing attacks, reducing the risk of initial compromise in targeted campaigns like TOITOIN.

Implement stringent access policies and enforce least privilege principles to prevent unauthorized access and contain the spread of malware within the organization's network.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	**TA0001** Initial Access	**TA0002** Execution	**TA0003** Persistence
TA0004 Privilege Escalation	**TA0005** Defense Evasion	**TA0007** Discovery	**TA0011** Command and Control
T1566 Phishing	**T1037** Boot or Logon Initialization Scripts	**T1055** Process Injection	**T1018** Remote System Discovery
T1082 System Information Discovery	**T1083** File and Directory Discovery	**T1548** Abuse Elevation Control Mechanism	**T1548.002** Bypass User Account Control
T1574 Hijack Execution Flow	**T1574.002** DLL Side-Loading	**T1055** Process Injection	**T1055.012** Process Hollowing
T1573 Encrypted Channel			

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	8fc3c83b88a3c65a749b27f8439a8416, 2fa7c647c626901321f5decde4273633, b7bc67f2ef833212f25ef58887d5035a, 690bfd65c2738e7c1c42ca8050634166, e6c7d8d5683f338ca5c40aad462263a6, c35d55b8b0ddd01aa4796d1616c09a46, 7871f9a0b4b9c413a8c7085983ec9a72
URLs	ec2-3-89-143-150[.]compute-1[.]amazonaws[.]com/storage[.]php?e=Desktop-PC, ec2-3-82-104-156[.]compute-1[.]amazonaws[.]com/storage.php?e=Desktop-PC, http[:]//alemaoautopecas[.]com, http[:]//contatosclientes[.]services, http[:]//cartolabrasil[.]com, http[:]//bragancasbrasil[.]com, http[:]//afroblack[.]shop/CasaMoveis\ClienteD.php
Domains	atendimento-arquivos[.]com, arquivosclientes[.]online, fantasiacinematica[.]online
IPv4	91[.]252[.]203[.]222, 179[.]188[.]38[.]7

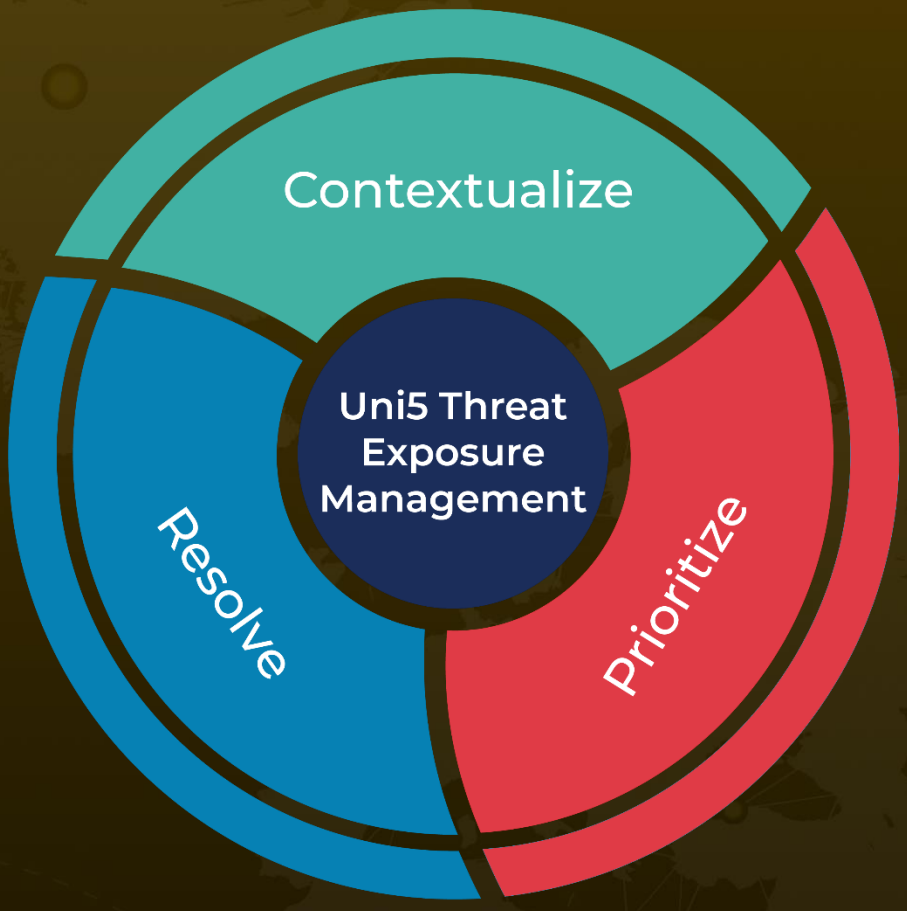
References

https://www.zscaler.com/blogs/security-research/toitoin-trojan-analyzing-new-multi-stage-attack-targeting-latam-region

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 11, 2023 • 7:00 AM

More at www.hivepro.com