Dec 14 2023

NETMANAGEIT

Intelligence Report

Mallox Resurrected: Ransomware Attacks Exploiting MS-SQL Continue to Burden Enterprises

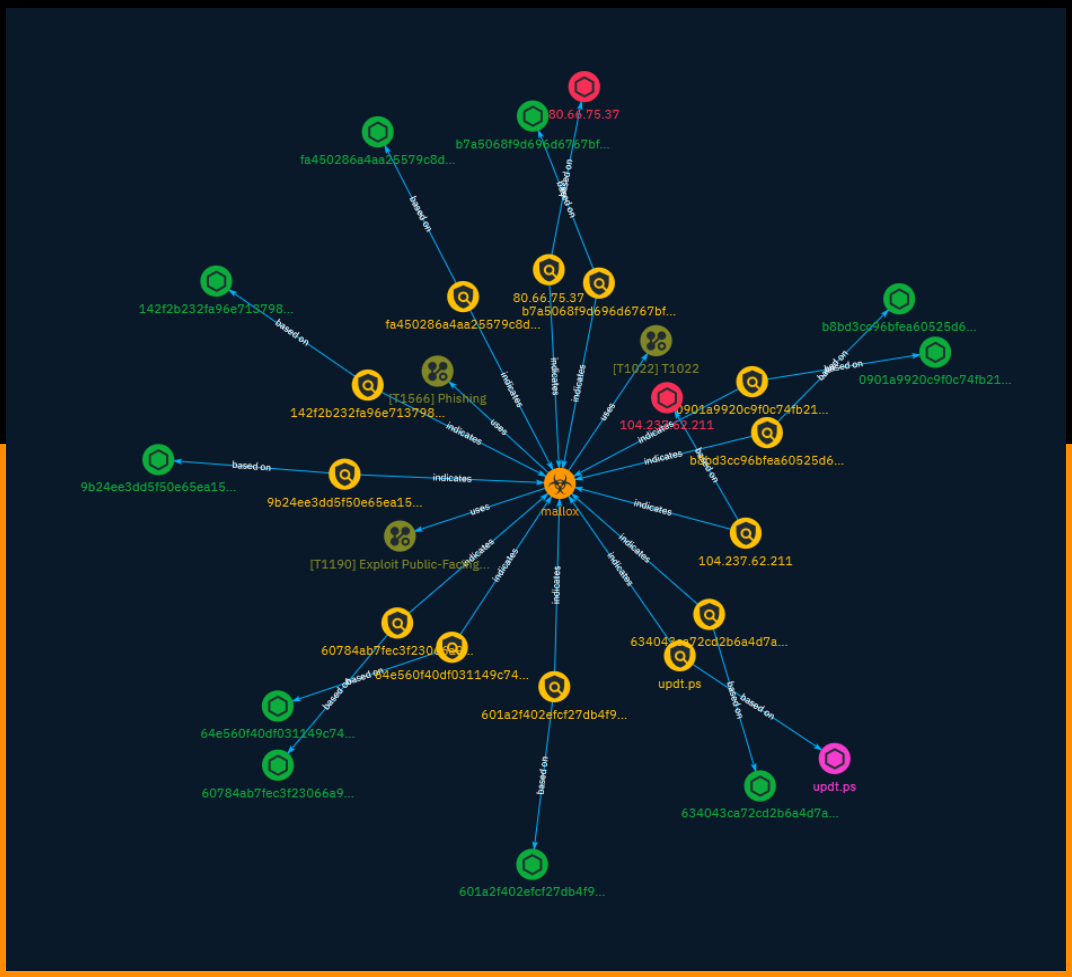

Table of contents

Overview

Entities

Observables

External References

Overview

Description

SentinelOne researchers disclosed a new blog on Mallox activity, explaining the group's initial access methods and providing a high-level analysis of recent Mallox payloads .

Confidence

This value represents the confidence in the correctness of the data contained within this report.

15 / 100

Content

N/A

Attack-Pattern

Name
Phishing
ID
T1566
Description
Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

Name

Exploit Public-Facing Application

ID

T1190

Description

Adversaries may attempt to exploit a weakness in an Internet-facing host or system to initially access a network. The weakness in the system can be a software bug, a temporary glitch, or a misconfiguration. Exploited applications are often websites/web servers, but can also include databases (like SQL), standard services (like SMB or SSH), network device administration and management protocols (like SNMP and Smart Install), and any other system with Internet accessible open sockets.(Citation: NVD CVE-2016-6662)(Citation: CIS Multiple SMB Vulnerabilities)(Citation: US-CERT TA18-106A Network Infrastructure Devices 2018)(Citation: Cisco Blog Legacy Device Attacks)(Citation: NVD CVE-2014-7169) Depending on the flaw being exploited this may also involve [Exploitation for Defense Evasion](https://attack.mitre.org/techniques/T1211). If an application is hosted on cloud-based infrastructure and/or is containerized, then exploiting it may lead to compromise of the underlying instance or container. This can allow an adversary a path to access the cloud or container APIs, exploit container host access via [Escape to Host](https://attack.mitre.org/techniques/T1611), or take advantage of weak identity and access management policies. Adversaries may also exploit edge network infrastructure and related appliances, specifically targeting devices that do not support robust host-based defenses.(Citation: Mandiant Fortinet Zero Day)(Citation: Wired Russia Cyberwar) For websites and databases, the OWASP top 10 and CWE top 25 highlight the most common web-based vulnerabilities. (Citation: OWASP Top 10)(Citation: CWE top 25)

Name

T1022

ID

T1022

Indicator

Name
b7a5068f9d696d6767bfddaea222649ff3541af306f93bce23c0aa6edd892534
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'b7a5068f9d696d6767bfddaea222649ff3541af306f93bce23c0aa6edd892534']
Name
9b24ee3dd5f50e65ea15aaa3946e76281c4f9d519524dc659f2bcdfb62241316
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '9b24ee3dd5f50e65ea15aaa3946e76281c4f9d519524dc659f2bcdfb62241316']
Name

80.66.75.37

Description

Remcos botnet C2 server (confidence level: 100%)

Pattern Type

stix

Pattern

[ipv4-addr:value = '80.66.75.37']

Name

64e560f40df031149c745ecaf44ce379aa44373d80a0ee3c4bd0abf7955df88e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '64e560f40df031149c745ecaf44ce379aa44373d80a0ee3c4bd0abf7955df88e']

Name

60784ab7fec3f23066a996f3347b721a09eb677b63dbc5e1bb2bfc920fa3f13d

Pattern Type

stix

Pattern
[file:hashes.'SHA-256' = '60784ab7fec3f23066a996f3347b721a09eb677b63dbc5e1bb2bfc920fa3f13d']
Name
104.237.62.211
Pattern Type
stix
Pattern
[ipv4-addr:value = '104.237.62.211']
Name
updt.ps
Pattern Type
stix
Pattern
[domain-name:value = 'updt.ps']
Name
142f2b232fa96e71379894d1bb6cb242c0f33886c1802922163901e70fdc3320
Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '142f2b232fa96e71379894d1bb6cb242c0f33886c1802922163901e70fdc3320']

Name

b8bd3cc96bfea60525d611e38b4de30c59d82d1df54a873fc9998533945063ff

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b8bd3cc96bfea60525d611e38b4de30c59d82d1df54a873fc9998533945063ff']

Name

601a2f402efcf27db4f9343a60e411959f92cdbb7802bbf4030df7b671c559e3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '601a2f402efcf27db4f9343a60e411959f92cdbb7802bbf4030df7b671c559e3']

Name

0901a9920c9f0c74fb2170524477693d62c8493715520ae95143abd8055e7a39

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0901a9920c9f0c74fb2170524477693d62c8493715520ae95143abd8055e7a39']

Name

634043ca72cd2b6a4d7a1cfe2aa12b7cd8c8348055fbc38c7d8006602ac66b87

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '634043ca72cd2b6a4d7a1cfe2aa12b7cd8c8348055fbc38c7d8006602ac66b87']

Name

fa450286a4aa25579c8da7684051e7cdda3ba249ff03da71689e5138fd9f5c73

Pattern Type

stix

Pattern

```
[file:hashes.'SHA-256' =
'fa450286a4aa25579c8da7684051e7cdda3ba249ff03da71689e5138fd9f5c73']
```

Malware

Name
mallox

Domain-Name

Value
updt.ps

StixFile

Value
634043ca72cd2b6a4d7a1cfe2aa12b7cd8c8348055fbc38c7d8006602ac66b87
64e560f40df031149c745ecaf44ce379aa44373d80a0ee3c4bd0abf7955df88e
fa450286a4aa25579c8da7684051e7cdda3ba249ff03da71689e5138fd9f5c73
60784ab7fec3f23066a996f3347b721a09eb677b63dbc5e1bb2bfc920fa3f13d
9b24ee3dd5f50e65ea15aaa3946e76281c4f9d519524dc659f2bcdfb62241316
0901a9920c9f0c74fb2170524477693d62c8493715520ae95143abd8055e7a39
b7a5068f9d696d6767bfddaea222649ff3541af306f93bce23c0aa6edd892534
b8bd3cc96bfea60525d611e38b4de30c59d82d1df54a873fc9998533945063ff
601a2f402efcf27db4f9343a60e411959f92cdbb7802bbf4030df7b671c559e3
142f2b232fa96e71379894d1bb6cb242c0f33886c1802922163901e70fdc3320

IPv4-Addr

Value
104.237.62.211
80.66.75.37

External References

- https://otx.alienvault.com/pulse/657b32b4adf944b8df50e72d
- https://www.sentinelone.com/blog/mallox-resurrected-ransomware-attacks-exploiting-ms-sql-continue-to-burden-enterprises/