Apr 14 2024

NETMANAGEIT

Intelligence Report

Persistent Magento backdoor hidden in XML

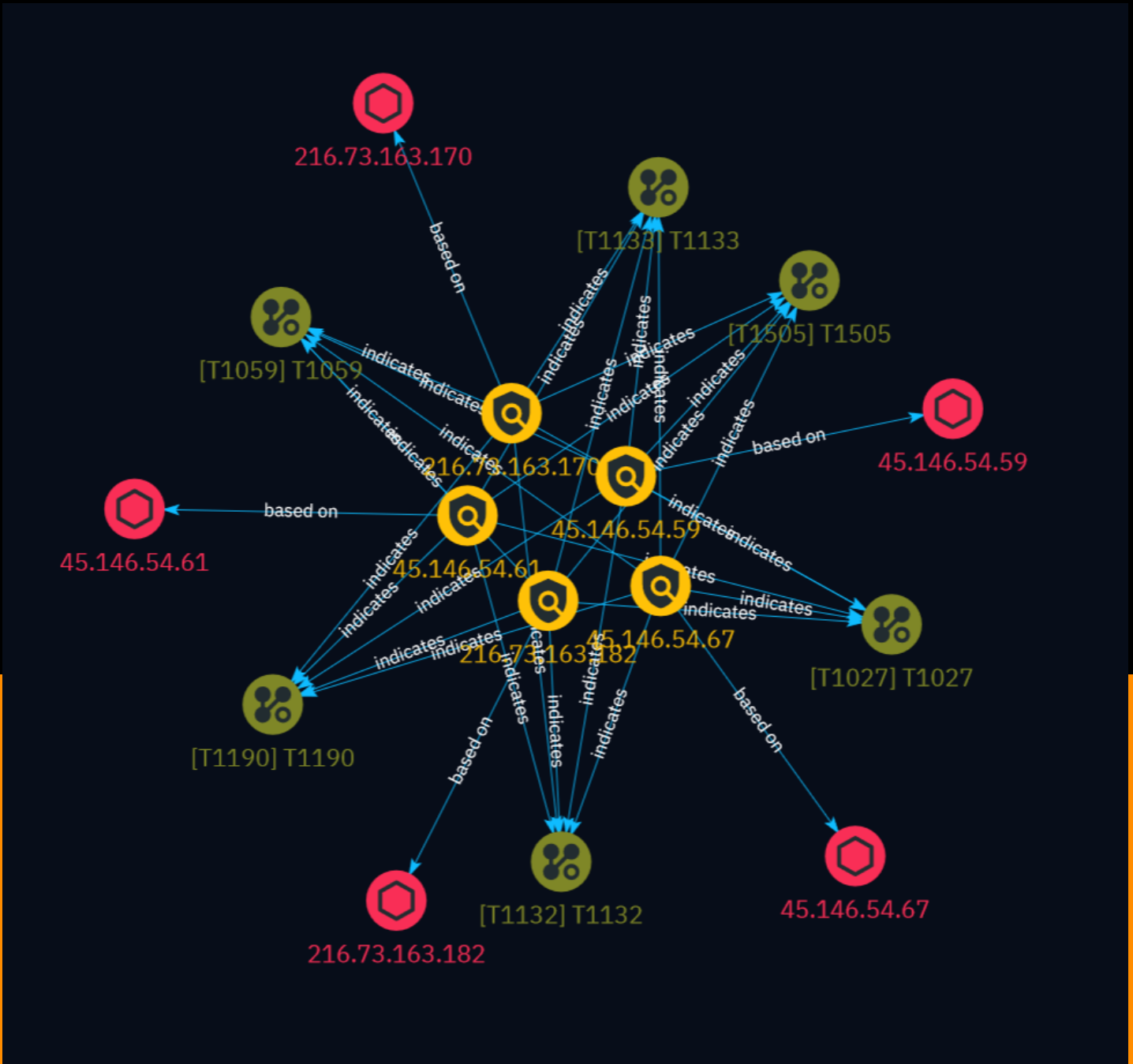

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Attackers are using a new method for malware persistence on Magento servers. Sansec discovered a cleverly crafted layout template in the database, which was used to automatically inject malware. The attackers combine the Magento layout parser with the beberlei/assert package to execute system commands, adding a backdoor to the CMS controller. This leads to a remote code execution backdoor which can be used to inject a fake Stripe payment skimmer.

Confidence

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

100 / 100

Content

N/A

Indicator

Name
45.146.54.67
Pattern Type
stix
Pattern
[ipv4-addr:value = '45.146.54.67']
Name
45.146.54.61
Pattern Type
stix
Pattern
[ipv4-addr:value = '45.146.54.61']
Name
45.146.54.59

Description

ISP: IPXO LIMITED **OS:** - ---------- Services: **6881:** ``` DHT Nodes 69.159.229.224 57108 58.210.181.25 10564 71.158.219.82 21656 23.207.37.53 40690 161.201.68.217 55752 203.118.64.206 31324 182.15.189.16 17652 184.90.172.227 24531 175.145.203.251 18348 144.32.42.36 1710 82.255.14.203 25015 163.140.204.104 4836 31.46.153.70 6881 70.5.64.70 12333 83.130.172.196 44023 130.103.234.182 28733 27.120.37.59 12945 26.225.65.143 18533 248.94.243.16 22906 249.17.34.246 21729 77.78.204.162 21777 172.94.200.213 17331 133.117.156.193 54513 216.192.1.110 16675 48.57.58.56 27701 109.252.220.68 1311 66.88.215.130 47708 201.248.185.124 21469 192.131.36.246 4098 154.248.46.10 38259 131.36.77.2 28134 109.183.52.228 35330 212.130.185.74 50178 225.78.107.86 11607 ``` ---------- **13899:** ``` DHT Nodes 120.172.160.81 62584 211.127.247.12 33640 140.153.54.131 58086 165.55.103.153 33525 245.186.123.0 33084 107.191.110.101 53006 102.246.224.85 4824 29.180.16.161 24488 167.199.109.112 31451 203.52.249.159 65113 142.17.86.137 39013 70.58.68.99 33058 72.53.226.146 16752 125.218.111.166 19698 146.199.183.110 26799 33.8.116.65 37944 183.109.178.71 17390 62.110.124.220 11965 16.78.42.57 46604 49.175.224.204 3593 222.124.233.104 54279 197.173.179.142 32590 20.19.13.137 2588 219.174.50.32 39504 238.64.120.54 64837 128.68.52.194 32109 126.119.179.57 58457 11.115.178.193 40104 156.164.84.156 44780 71.164.221.114 13414 84.126.113.42 39525 167.177.242.90 19216 187.197.57.237 11266 12.159.188.141 1415 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.146.54.59']

Name

216.73.163.182

Pattern Type

stix

Pattern

[ipv4-addr:value = '216.73.163.182']

Name

216.73.163.170

Pattern Type

stix

Pattern

[ipv4-addr:value = '216.73.163.170']

Attack-Pattern

Name
T1505
ID
T1505
Description
Adversaries may abuse legitimate extensible development features of servers to establish persistent access to systems. Enterprise server applications may include features that allow developers to write and install software or scripts to extend the functionality of the main application. Adversaries may install malicious components to extend and abuse server applications.(Citation: volexity_0day_sophos_FW)
Name
T1132
ID
T1132
Description
Adversaries may encode data to make the content of command and control traffic more difficult to detect. Command and control (C2) information can be encoded using a standard data encoding system. Use of data encoding may adhere to existing protocol

specifications and includes use of ASCII, Unicode, Base64, MIME, or other binary-to-text and character encoding systems.(Citation: Wikipedia Binary-to-text Encoding) (Citation: Wikipedia Character Encoding) Some data encoding systems may also result in data compression, such as gzip.

Name

T1059

ID

T1059

Description

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of [Unix Shell](https://attack.mitre.org/techniques/T1059/004) while Windows installations include the [Windows Command Shell](https://attack.mitre.org/techniques/T1059/003) and [PowerShell](https://attack.mitre.org/techniques/T1059/001). There are also cross-platform interpreters such as [Python](https://attack.mitre.org/techniques/T1059/006), as well as those commonly associated with client applications such as [JavaScript](https://attack.mitre.org/techniques/T1059/007) and [Visual Basic](https://attack.mitre.org/techniques/T1059/005). Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in [Initial Access](https://attack.mitre.org/tactics/TA0001) payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various [Remote Services](https://attack.mitre.org/techniques/T1021) in order to achieve remote Execution. (Citation: Powershell Remote Commands)(Citation: Cisco IOS Software Integrity Assurance - Command History)(Citation: Remote Shell Execution in Python)

Name

T1027

ID

T1027

Description

Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses. Payloads may be compressed, archived, or encrypted in order to avoid detection. These payloads may be used during Initial Access or later to mitigate detection. Sometimes a user's action may be required to open and [Deobfuscate/Decode Files or Information](https://attack.mitre.org/techniques/T1140) for [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016) Adversaries may also use compressed or archived scripts, such as JavaScript. Portions of files can also be encoded to hide the plain-text strings that would otherwise help defenders with discovery. (Citation: Linux/Cdorked.A We Live Security Analysis) Payloads may also be split into separate, seemingly benign files that only reveal malicious functionality when reassembled. (Citation: Carbon Black Obfuscation Sept 2016) Adversaries may also abuse [Command Obfuscation](https://attack.mitre.org/techniques/T1027/010) to obscure commands executed from payloads or directly via [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059). Environment variables, aliases, characters, and other platform/language specific semantics can be used to evade signature based detections and application control mechanisms. (Citation: FireEye Obfuscation June 2017) (Citation: FireEye Revoke-Obfuscation July 2017)(Citation: PaloAlto EncodedCommand March 2017)

Name

T1190

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

T1133

ID

T1133

Description

Adversaries may leverage external-facing remote services to initially access and/or persist within a network. Remote services such as VPNs, Citrix, and other access mechanisms allow users to connect to internal enterprise network resources from external locations. There are often remote service gateways that manage connections and credential authentication for these services. Services such as [Windows Remote Management](https://attack.mitre.org/techniques/T1021/006) and [VNC](https://attack.mitre.org/techniques/T1021/005) can also be used externally.(Citation: MacOS VNC software for Remote Desktop) Access to [Valid Accounts](https://attack.mitre.org/techniques/T1078) to use the service is often a requirement, which could be obtained through credential pharming or by obtaining the credentials from users after compromising the enterprise

network.(Citation: Volexity Virtual Private Keylogging) Access to remote services may be used as a redundant or persistent access mechanism during an operation. Access may also be gained through an exposed service that doesn't require authentication. In containerized environments, this may include an exposed Docker API, Kubernetes API server, kubelet, or web application such as the Kubernetes dashboard.(Citation: Trend Micro Exposed Docker Server)(Citation: Unit 42 Hildegard Malware)

IPv4-Addr

Value
45.146.54.67
45.146.54.61
45.146.54.59
216.73.163.182
216.73.163.170

External References

- https://sansec.io/research/magento-xml-backdoor
- https://otx.alienvault.com/pulse/6616d15907e0bbe3c1572c4c