Aug 08 2023

NETMANAGEIT

Intelligence Report

VMConnect: Malicious PyPI packages imitate popular open source modules

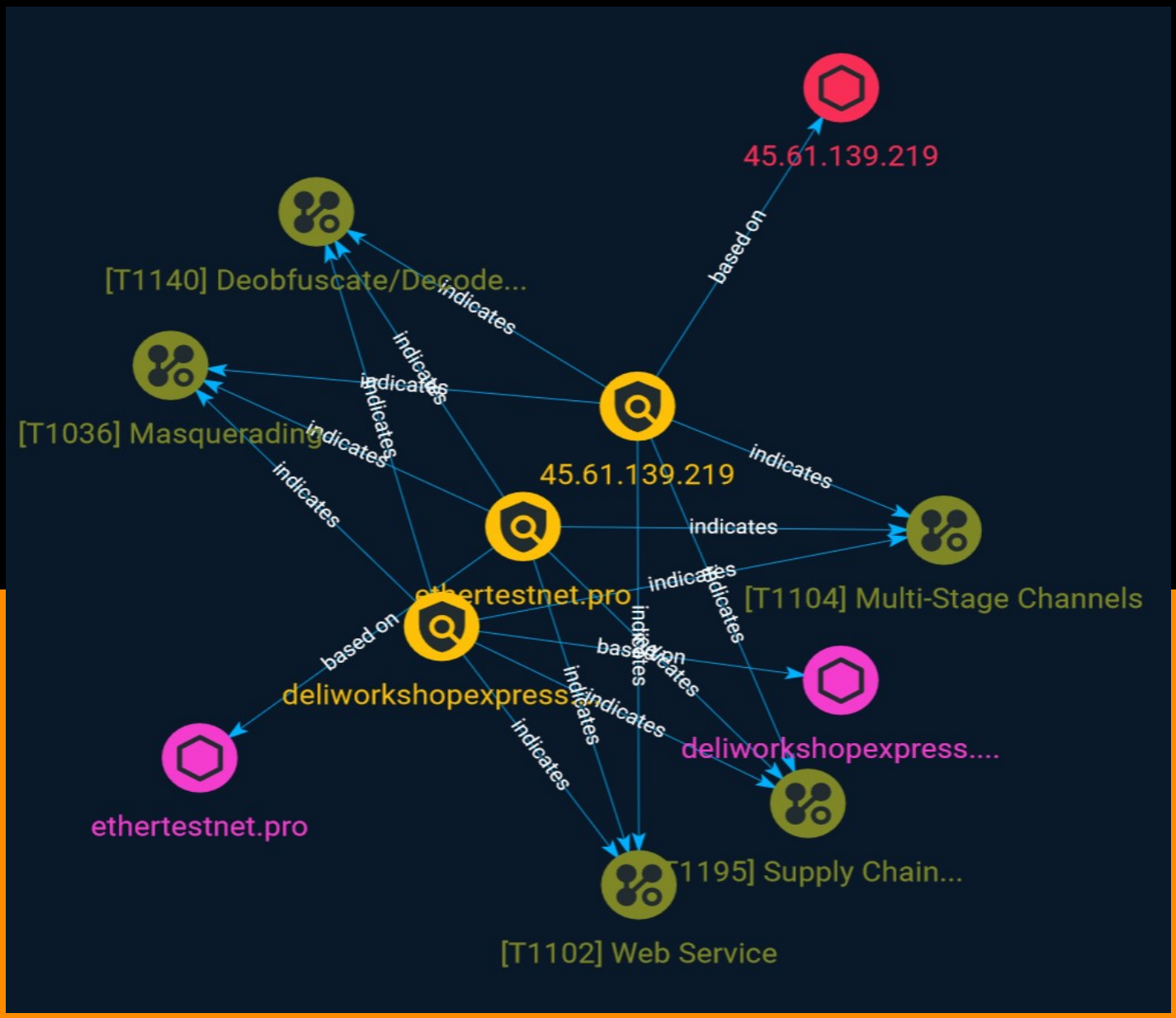

Table of contents

Overview

- Description 3
- Confidence 3

Entities

- Indicator 4
- Attack-Pattern 6

Observables

- Domain-Name 10
- IPv4-Addr 11

External References

- External References 12

Overview

Description

Software supply chain security researchers from ReversingLabs have identified a campaign of malicious Python packages imitating popular open source tools, which they believe could be used to plant malicious code for the next three years.

Confidence

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

15 / 100

Indicator

Name
ethertestnet.pro
Pattern Type
stix
Pattern
[domain-name:value = 'ethertestnet.pro']
Name
deliworkshopexpress.xyz
Pattern Type
stix
Pattern
[domain-name:value = 'deliworkshopexpress.xyz']
Name
45.61.139.219

Description

ISP: BL Networks **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.2 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQC2OEVlaUV8PXBBEy6Cc7heltRQoN3OBBc2Iz9TUnc/KXYo lppQ2FIsOm0jUpqGJxn0LaHaL+tR5AifR/ZvU9ddRtOnXD63SYP2Lc82GF3mayTgoMq+Km2bao3z 85aaX3bUZC7iC9BvkgZisonnKZSlG490mAFUDzHLs4EuoYRhnQ/lP14ZsPwoxN5WuvD9PpcTKwuc RVGKzyuCUbnl3mFWh1Fb7T2lCMhur/PlstZURoCuSneE87W2uX0h6/4mLI3dEo8hBB54PqRXmacB 1tPSprzaTjAbNT1zzatJBs059HUzV15RNqtennnMNIZpj+iHCJo1kkc8Btfa0lRT5jT6ptci+SDC2 9mRVdRKPVkU2BbG1cYBeJtL56tw+c8tLqMa5LBopZ5xGRtJ12NWd1INL6/ov2NDFJipHMX7W2FLi O5t864y/xRr1+ZupOQ7XOLbjtOOJl/F4oxr1z8LqvvQCwgRcsiacs1CBGP+gNMAJUjJo1IEnfV20 +ZMO6cQH000= Fingerprint: 90:38:74:8c:9f:99:15:d8:80:3b:81:7e:a9:f9:4b:7a Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ssh-rsa ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ``` ---------- **80:** ``` HTTP/1.1 200 OK Date: Tue, 01 Aug 2023 21:31:46 GMT Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.0.28 Last-Modified: Thu, 06 Apr 2023 09:24:30 GMT ETag: "1443-5f8a779c90f80" Accept-Ranges: bytes Content-Length: 5187 Content-Type: text/html ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.61.139.219']

Attack-Pattern

Name

Supply Chain Compromise

ID

T1195

Description

Adversaries may manipulate products or product delivery mechanisms prior to receipt by a final consumer for the purpose of data or system compromise. Supply chain compromise can take place at any stage of the supply chain including: * Manipulation of development tools * Manipulation of a development environment * Manipulation of source code repositories (public or private) * Manipulation of source code in open-source dependencies * Manipulation of software update/distribution mechanisms * Compromised/infected system images (multiple cases of removable media infected at the factory)(Citation: IBM Storwize)(Citation: Schneider Electric USB Malware) * Replacement of legitimate software with modified versions * Sales of modified/counterfeit products to legitimate distributors * Shipment interdiction While supply chain compromise can impact any component of hardware or software, adversaries looking to gain execution have often focused on malicious additions to legitimate software in software distribution or update channels.(Citation: Avast CCleaner3 2018)(Citation: Microsoft Dofoil 2018)(Citation: Command Five SK 2011) Targeting may be specific to a desired victim set or malicious software may be distributed to a broad set of consumers but only move on to additional tactics on specific victims.(Citation: Symantec Elderwood Sept 2012)(Citation: Avast CCleaner3 2018)(Citation: Command Five SK 2011) Popular open source projects that are used as dependencies in many applications may also be targeted as a means to add malicious code to users of the dependency.(Citation: Trendmicro NPM Compromise)

Name

Masquerading

ID

T1036

Description

Adversaries may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools. Masquerading occurs when the name or location of an object, legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation. This may include manipulating file metadata, tricking users into misidentifying the file type, and giving legitimate task or service names. Renaming abusable system utilities to evade security monitoring is also a form of [Masquerading](https://attack.mitre.org/techniques/T1036).(Citation: LOLBAS Main Site)

Name

Multi-Stage Channels

ID

T1104

Description

Adversaries may create multiple stages for command and control that are employed under different conditions or for certain functions. Use of multiple stages may obfuscate the command and control channel to make detection more difficult. Remote access tools will call back to the first-stage command and control server for instructions. The first stage may have automated capabilities to collect basic host information, update tools, and upload additional files. A second remote access tool (RAT) could be uploaded at that point to redirect the host to the second-stage command and control server. The second stage will likely be more fully featured and allow the adversary to interact with the system through a reverse shell and additional RAT features. The different stages will likely be hosted separately with no overlapping infrastructure. The loader may also have backup

first-stage callbacks or [Fallback Channels](https://attack.mitre.org/techniques/T1008) in case the original first-stage communication path is discovered and blocked.

Name

Web Service

ID

T1102

Description

Adversaries may use an existing, legitimate external Web service as a means for relaying data to/from a compromised system. Popular websites and social media acting as a mechanism for C2 may give a significant amount of cover due to the likelihood that hosts within a network are already communicating with them prior to a compromise. Using common services, such as those offered by Google or Twitter, makes it easier for adversaries to hide in expected noise. Web service providers commonly use SSL/TLS encryption, giving adversaries an added level of protection. Use of Web services may also protect back-end C2 infrastructure from discovery through malware binary analysis while also enabling operational resiliency (since this infrastructure may be dynamically changed).

Name

Deobfuscate/Decode Files or Information

ID

T1140

Description

Adversaries may use [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027) to hide artifacts of an intrusion from analysis. They may require separate mechanisms to decode or deobfuscate that information depending on how they intend to use it. Methods for doing that include built-in functionality of malware or by

using utilities present on the system. One such example is the use of [certutil](https://attack.mitre.org/software/S0160) to decode a remote access tool portable executable file that has been hidden inside a certificate file.(Citation: Malwarebytes Targeted Attack against Saudi Arabia) Another example is using the Windows `copy /b` command to reassemble binary fragments into a malicious payload.(Citation: Carbon Black Obfuscation Sept 2016) Sometimes a user's action may be required to open it for deobfuscation or decryption as part of [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)

Domain-Name

Value
deliworkshopexpress.xyz
ethertestnet.pro

IPv4-Addr

Value
45.61.139.219

External References

- https://otx.alienvault.com/pulse/64d26652e33287d2d5ca7fe7
- https://www.reversinglabs.com/blog/vmconnect-malicious-pypi-packages-imitate-popular-open-source-modules