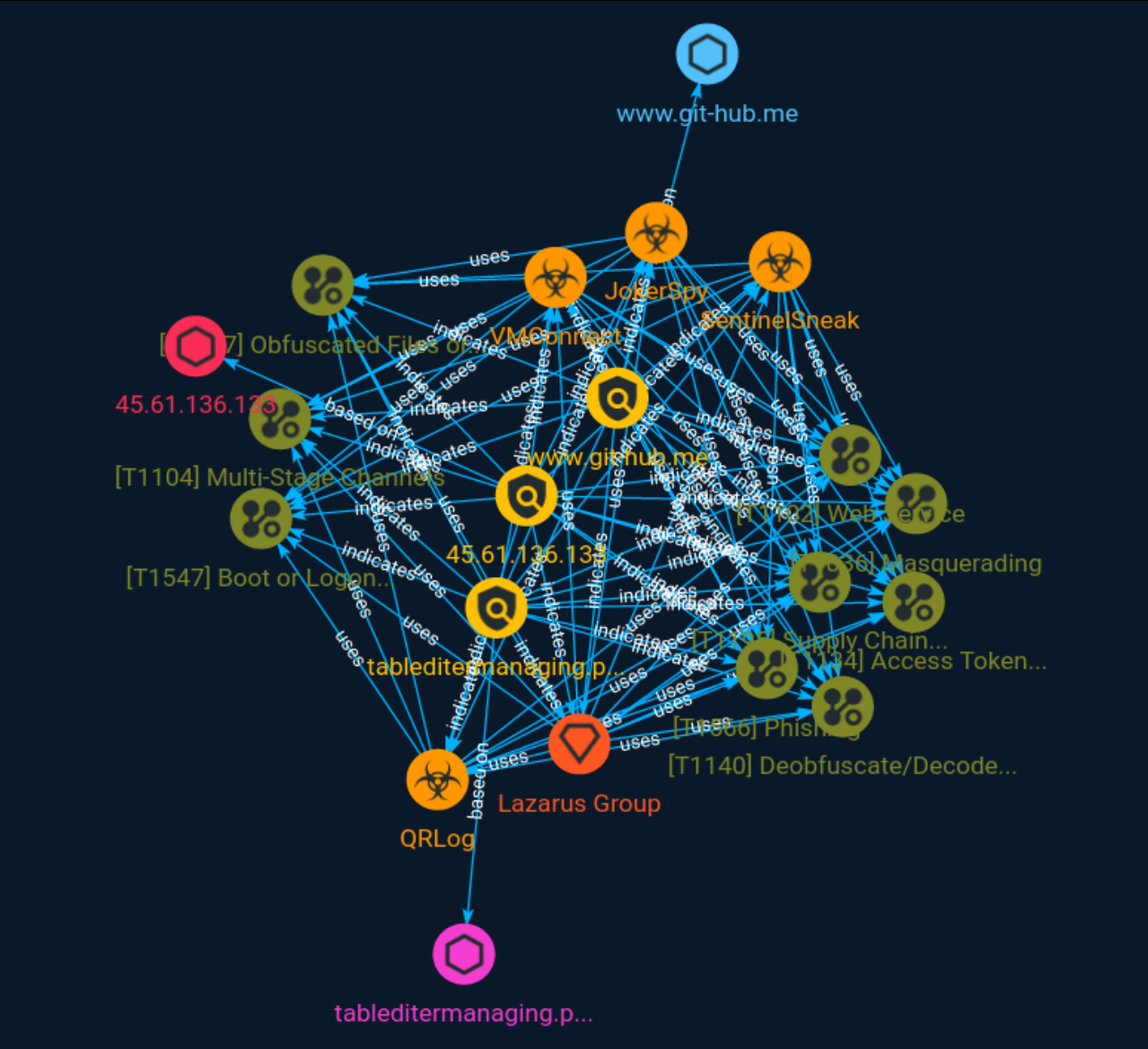




NETMANAGEIT

# Intelligence Report

## VMConnect supply chain attack continues, evidence points to North Korea



# Table of contents

---

## Overview

---

● Description	4
● Confidence	4

---

---

## Entities

---

● Indicator	5
● Malware	7
● Attack-Pattern	8
● Intrusion-Set	15

---

---

## Observables

---

● Domain-Name	16
● IPv4-Addr	17
● Hostname	18

---



## External References

- External References

19

# Overview

## Description

Researchers have identified a new group of malicious Python packages that appear to be a continuation of the VMConnect supply chain attack, which was carried out by North Korean state-sponsored hackers.

## Confidence

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

15 / 100

# Indicator

## Name

45.61.136.133

## Description

```

**ISP:** BL Networks **OS:** Windows (build 10.0.19041) -----
Hostnames: - tableditermanaging.pro ----- Domains: -
tableditermanaging.pro ----- Services: **80:** HTTP/1.1 403 Forbidden
Date: Fri, 01 Sep 2023 06:17:23 GMT Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.0.28
Content-Length: 303 Content-Type: text/html; charset=iso-8859-1 ~~~ -----
**443:** HTTP/1.1 403 Forbidden Date: Thu, 31 Aug 2023 23:10:01 GMT Server: Apache/2.4.56
(Win64) OpenSSL/1.1.1t PHP/8.0.28 Content-Length: 304 Content-Type: text/html;
charset=iso-8859-1 ~~~ HEARTBLEED: 2023/08/31 23:10:08 45.61.136.133:443 - SAFE
----- **3389:** Remote Desktop Protocol
\x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x1f\x08\x00\x02\x00\x00\x00 Remote
Desktop Protocol NTLM Info: OS: Windows 10 (version 2004)/Windows Server (version 2004)
OS Build: 10.0.19041 Target Name: 64CC723F0805472 NetBIOS Domain Name:
64CC723F0805472 NetBIOS Computer Name: 64CC723F0805472 DNS Domain Name:
64cc723f0805472 FQDN: 64cc723f0805472 ~~~ -----

```

## Pattern Type

stix

## Pattern

[ipv4-addr:value = '45.61.136.133']

**Name**

tableditermanaging.pro

**Pattern Type**

stix

**Pattern**

[domain-name:value = 'tableditermanaging.pro']

**Name**

www.git-hub.me

**Pattern Type**

stix

**Pattern**

[hostname:value = 'www.git-hub.me']

# Malware

**Name**

VMConnect

**Name**

SentinelSneak

**Name**

QRLog

**Name**

JokerSpy

# 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 Dofail 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**

Boot or Logon Autostart Execution

**ID**

T1547

**Description**

Adversaries may configure system settings to automatically execute a program during system boot or logon to maintain persistence or gain higher-level privileges on compromised systems. Operating systems may have mechanisms for automatically running a program on system boot or account logon.(Citation: Microsoft Run Key)(Citation: MSDN Authentication Packages)(Citation: Microsoft TimeProvider)(Citation: Cylance Reg Persistence Sept 2013)(Citation: Linux Kernel Programming) These mechanisms may include automatically executing programs that are placed in specially designated directories or are referenced by repositories that store configuration information, such as the Windows Registry. An adversary may achieve the same goal by modifying or extending features of the kernel. Since some boot or logon autostart programs run with higher privileges, an adversary may leverage these to elevate privileges.

**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**

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**

Obfuscated Files or Information

**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**

Access Token Manipulation

**ID**

T1134

**Description**

Adversaries may modify access tokens to operate under a different user or system security context to perform actions and bypass access controls. Windows uses access tokens to determine the ownership of a running process. A user can manipulate access tokens to

make a running process appear as though it is the child of a different process or belongs to someone other than the user that started the process. When this occurs, the process also takes on the security context associated with the new token. An adversary can use built-in Windows API functions to copy access tokens from existing processes; this is known as token stealing. These token can then be applied to an existing process (i.e. [Token Impersonation/Theft](https://attack.mitre.org/techniques/T1134/001)) or used to spawn a new process (i.e. [Create Process with Token](https://attack.mitre.org/techniques/T1134/002)). An adversary must already be in a privileged user context (i.e. administrator) to steal a token. However, adversaries commonly use token stealing to elevate their security context from the administrator level to the SYSTEM level. An adversary can then use a token to authenticate to a remote system as the account for that token if the account has appropriate permissions on the remote system.(Citation: Pentestlab Token Manipulation) Any standard user can use the ``runas`` command, and the Windows API functions, to create impersonation tokens; it does not require access to an administrator account. There are also other mechanisms, such as Active Directory fields, that can be used to modify access tokens.

**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)

# Intrusion-Set

## Name

Lazarus Group

## Description

[Lazarus Group](<https://attack.mitre.org/groups/G0032>) is a North Korean state-sponsored cyber threat group that has been attributed to the Reconnaissance General Bureau. (Citation: US-CERT HIDDEN COBRA June 2017)(Citation: Treasury North Korean Cyber Groups September 2019) The group has been active since at least 2009 and was reportedly responsible for the November 2014 destructive wiper attack against Sony Pictures Entertainment as part of a campaign named Operation Blockbuster by Novetta. Malware used by [Lazarus Group](<https://attack.mitre.org/groups/G0032>) correlates to other reported campaigns, including Operation Flame, Operation 1Mission, Operation Troy, DarkSeoul, and Ten Days of Rain. (Citation: Novetta Blockbuster) North Korean group definitions are known to have significant overlap, and some security researchers report all North Korean state-sponsored cyber activity under the name [Lazarus Group](<https://attack.mitre.org/groups/G0032>) instead of tracking clusters or subgroups, such as [Andariel](<https://attack.mitre.org/groups/G0138>), [APT37](<https://attack.mitre.org/groups/G0067>), [APT38](<https://attack.mitre.org/groups/G0082>), and [Kimsuky](<https://attack.mitre.org/groups/G0094>).

# Domain-Name

## Value

tableditermanaging.pro



# IPv4-Addr

## Value

45.61.136.133

# Hostname

## Value

www.git-hub.me

# External References

- 
- <https://otx.alienvault.com/pulse/64f1eb1a539f7386b6847193>
- 
- <https://securityboulevard.com/2023/08/vmconnect-supply-chain-attack-continues-evidence-points-to-north-korea/>