Apr 05 2024

NETMANAGEIT

Intelligence Report

Distinctive Campaign Evolution of Malware

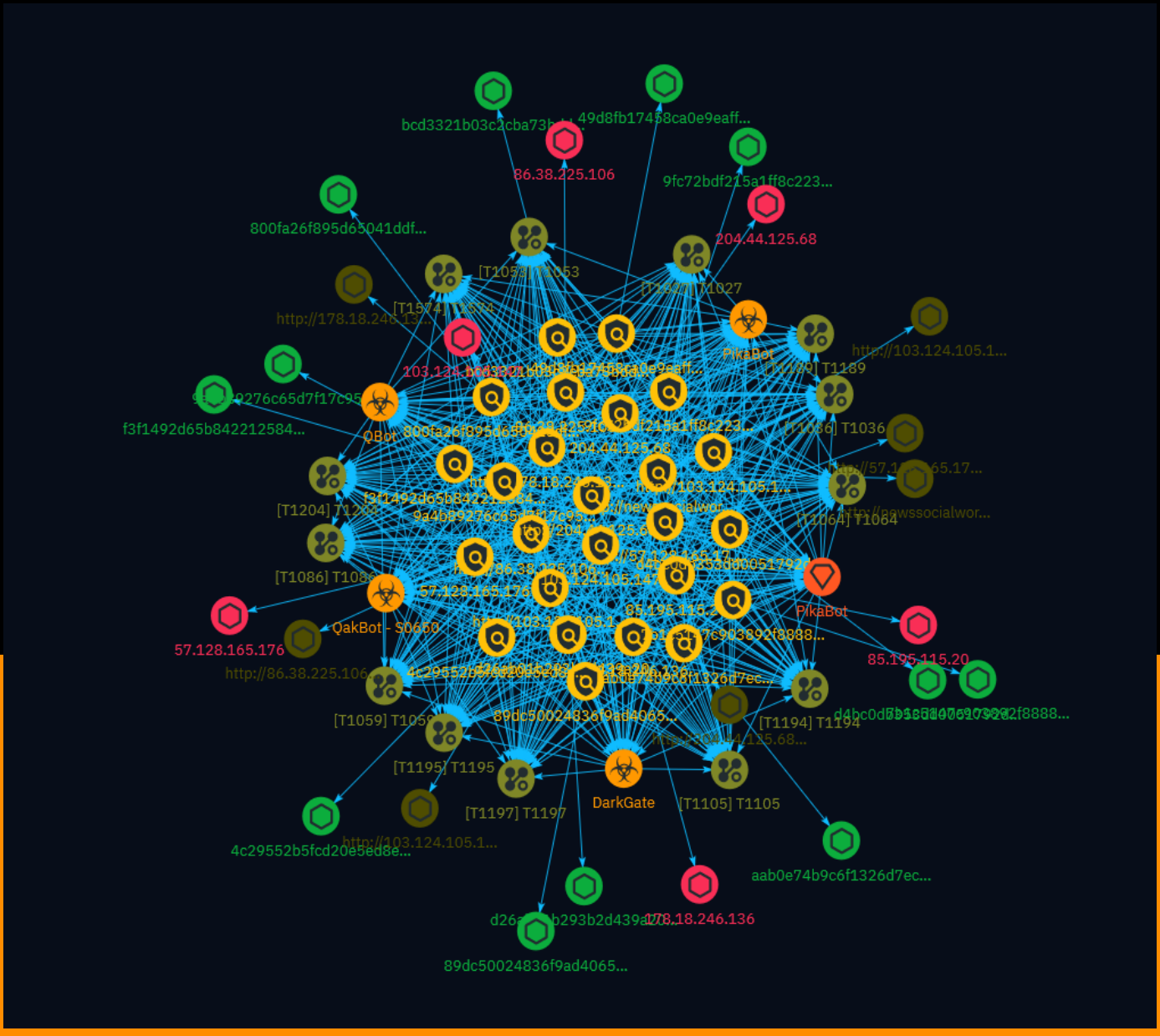

Table of contents

Overview

Entities

Observables

External References

Overview

Description

This report provides an analysis of the rapidly evolving campaigns employed by the threat actors behind the Pikabot malware, a malicious backdoor active since early 2023. Highlighting the diverse distribution methods utilized, including email spam campaigns with geographically targeted content, the report delves into the various file types leveraged as infection vectors, such as HTML, JavaScript, SMB shares, Excel documents, and JAR files. The report meticulously examines the infection chains, code snippets, and payloads associated with each campaign, underscoring the adversaries' relentless efforts to evade detection and successfully deliver the Pikabot payload.

Confidence

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

100 / 100

Content

N/A

Indicator

Name

http://newssocialwork.com/public/FNFY.zip

Description

- **Unsafe:** True - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** True - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** Web Tracker - **Domain Age:** {'human': '2 months ago', 'timestamp': 1708094334, 'iso': '2024-02-16T09:38:54-05:00'} - **IPQS: Domain:** newssocialwork.com - **IPQS: IP Address:** 66.63.168.90

Pattern Type

stix

Pattern

[url:value = 'http://newssocialwork.com/public/FNFY.zip']

Name

http://86.38.225.106:2221

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': 'N/

A', 'timestamp': None, 'iso': None} - **IPQS: Domain:** 86.38.225.106 - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://86.38.225.106:2221']

Name

http://204.44.125.68/mcqef/yPXpC.xn--txt-to0a.

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': 'N/A', 'timestamp': None, 'iso': None} - **IPQS: Domain:** 204.44.125.68 - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://204.44.125.68/mcqef/yPXpC.xn--txt-to0a.']

Name

http://57.128.165.176:1372

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': 'N/A', 'timestamp': None, 'iso': None} - **IPQS: Domain:** 57.128.165.176 - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://57.128.165.176:1372']

Name

http://178.18.246.136:2078

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': 'N/A', 'timestamp': None, 'iso': None} - **IPQS: Domain:** 178.18.246.136 - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://178.18.246.136:2078']

Name

http://103.124.105.147/KNaDVX/0.2642713404338389.dat

Pattern Type

stix

Pattern

[url:value = 'http://103.124.105.147/KNaDVX/0.2642713404338389.dat']

Name

http://103.124.105.147/KNaDVX/.xn--dat-9o0a

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': 'N/A', 'timestamp': None, 'iso': None} - **IPQS: Domain:** 103.124.105.147 - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://103.124.105.147/KNaDVX/.xn--dat-9o0a']

Name

86.38.225.106

Description

ISP: Majestic Hosting Solutions, LLC **OS:** Windows Server 2016 (version 1607) (build 10.0.14393) ---------- Services: **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 1607)/Windows Server 2016 (version 1607) OS Build: 10.0.14393 Target Name: WIN-860H0ABSUPR NetBIOS Domain Name: WIN-860H0ABSUPR NetBIOS Computer Name: WIN-860H0ABSUPR DNS Domain Name: WIN-860H0ABSUPR FQDN: WIN-860H0ABSUPR ; Administrator SES ``` ---------- **5985:** ``` HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Tue, 02 Apr 2024 06:00:11 GMT Connection: close Content-Length: 315 WinRM NTLM Info: OS: Windows Server 2016 (version 1607) OS Build: 10.0.14393 Target Name: WIN-860H0ABSUPR NetBIOS Domain Name: WIN-860H0ABSUPR NetBIOS Computer Name: WIN-860H0ABSUPR DNS Domain Name: WIN-860H0ABSUPR FQDN: WIN-860H0ABSUPR ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '86.38.225.106']

Name

85.195.115.20

Description

- **Zip Code:** N/A - **ISP:** velia.net Internetdienste - **ASN:** 20773 - **Organization:** Host Europe - **Is Crawler:** False - **Timezone:** Europe/Berlin - **Mobile:** False - **Host:** 85.195.115.20 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** DE - **Region:** Hesse - **City:** Frankfurt am Main - **Latitude:** 50.12 - **Longitude:** 8.68

Pattern Type

stix

Pattern

[ipv4-addr:value = '85.195.115.20']

Name

57.128.165.176

Description

ISP: OVH SAS **OS:** - ---------- Services: **8080:** ``` HTTP/1.1 200 OK Server: nginx Date: Tue, 02 Apr 2024 14:22:41 GMT Content-Type: text/html; charset=UTF-8 Connection: close ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '57.128.165.176']

Name

204.44.125.68

Description

ISP: QuadraNet Enterprises LLC **OS:** - ---------- Services: **80:** ``` HTTP/1.1 200 OK Date: Tue, 12 Mar 2024 18:29:11 GMT Server: Apache/2.4.41 (Ubuntu) Last-Modified: Thu, 22 Feb 2024 11:20:50 GMT ETag: "2aa6-611f6a2c92d0e" Accept-Ranges: bytes Content-Length: 10918 Vary: Accept-Encoding Content-Type: text/html ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '204.44.125.68']

Name

178.18.246.136

Description

ISP: Contabo GmbH **OS:** Windows Server 2022 (build 10.0.20348) ---------- Services: **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 Server 2022 OS Build: 10.0.20348 Target Name: TINY-379D18F3 NetBIOS Domain Name: TINY-379D18F3 NetBIOS Computer Name: TINY-379D18F3 DNS Domain Name: TINY-379D18F3 FQDN: TINY-379D18F3 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '178.18.246.136']

Name

f3f1492d65b8422125846728b320681baa05a6928fbbd25b16fa28b352b1b512

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f3f1492d65b8422125846728b320681baa05a6928fbbd25b16fa28b352b1b512']

Name

d4bc0db353dd0051792dd1bfd5a286d3f40d735e21554802978a97599205bd04

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd4bc0db353dd0051792dd1bfd5a286d3f40d735e21554802978a97599205bd04']

Name

d26ab01b293b2d439a20d1dffc02a5c9f2523446d811192836e26d370a34d1b4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd26ab01b293b2d439a20d1dffc02a5c9f2523446d811192836e26d370a34d1b4']

Name

bcd3321b03c2cba73bddca46c8a509096083e428b81e88ed90b0b7d4bd3ba4f5

Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'bcd3321b03c2cba73bddca46c8a509096083e428b81e88ed90b0b7d4bd3ba4f5']
Name
aab0e74b9c6f1326d7ecea9a0de137c76d52914103763ac6751940693f26cbb1
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'aab0e74b9c6f1326d7ecea9a0de137c76d52914103763ac6751940693f26cbb1']
Name
9a4b89276c65d7f17c9568db5e5744ed94244be7ab222bedd8b64f25695ef849
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '9a4b89276c65d7f17c9568db5e5744ed94244be7ab222bedd8b64f25695ef849']

Name

9fc72bdf215a1ff8c22354aac4ad3c19b98a115e448cb60e1b9d3948af580c82

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9fc72bdf215a1ff8c22354aac4ad3c19b98a115e448cb60e1b9d3948af580c82']

Name

89dc50024836f9ad406504a3b7445d284e97ec5dafdd8f2741f496cac84ccda9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '89dc50024836f9ad406504a3b7445d284e97ec5dafdd8f2741f496cac84ccda9']

Name

800fa26f895d65041ddf12c421b73eea7f452d32753f4972b05e6b12821c863a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '800fa26f895d65041ddf12c421b73eea7f452d32753f4972b05e6b12821c863a']

Name

7b1c5147c903892f8888f91c98097c89e419ddcc89958a33e294e6dd192b6d4e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7b1c5147c903892f8888f91c98097c89e419ddcc89958a33e294e6dd192b6d4e']

Name

4c29552b5fcd20e5ed8ec72dd345f2ea573e65412b65c99d897761d97c35ebfd

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4c29552b5fcd20e5ed8ec72dd345f2ea573e65412b65c99d897761d97c35ebfd']

Name

49d8fb17458ca0e9eaff8e3b9f059a9f9cf474cc89190ba42ff4f1e683e09b72

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '49d8fb17458ca0e9eaff8e3b9f059a9f9cf474cc89190ba42ff4f1e683e09b72']

Name

103.124.105.147

Description

- **Zip Code:** N/A - **ISP:** Hosteons - **ASN:** 142036 - **Organization:** Hosteons - **Is Crawler:** False - **Timezone:** America/Chicago - **Mobile:** False - **Host:** 103.124.105.147 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** True - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** US - **Region:** Texas - **City:** Dallas - **Latitude:** 32.78 - **Longitude:** -96.8

Pattern Type

stix

Pattern

[ipv4-addr:value = '103.124.105.147']

Attack-Pattern

Name
T1194
ID
T1194
Name
T1086
ID
T1086
Name
T1189
ID
T1189
Description
Adversaries may gain access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is typically targeted for

exploitation, but adversaries may also use compromised websites for non-exploitation behavior such as acquiring [Application Access Token](https://attack.mitre.org/techniques/T1550/001). Multiple ways of delivering exploit code to a browser exist (i.e., [Drive-by Target](https://attack.mitre.org/techniques/T1608/004)), including: * A legitimate website is compromised where adversaries have injected some form of malicious code such as JavaScript, iFrames, and cross-site scripting * Script files served to a legitimate website from a publicly writeable cloud storage bucket are modified by an adversary * Malicious ads are paid for and served through legitimate ad providers (i.e., [Malvertising](https://attack.mitre.org/techniques/T1583/008)) * Built-in web application interfaces are leveraged for the insertion of any other kind of object that can be used to display web content or contain a script that executes on the visiting client (e.g. forum posts, comments, and other user controllable web content). Often the website used by an adversary is one visited by a specific community, such as government, a particular industry, or region, where the goal is to compromise a specific user or set of users based on a shared interest. This kind of targeted campaign is often referred to a strategic web compromise or watering hole attack. There are several known examples of this occurring.(Citation: Shadowserver Strategic Web Compromise) Typical drive-by compromise process: 1. A user visits a website that is used to host the adversary controlled content. 2. Scripts automatically execute, typically searching versions of the browser and plugins for a potentially vulnerable version. * The user may be required to assist in this process by enabling scripting or active website components and ignoring warning dialog boxes. 3. Upon finding a vulnerable version, exploit code is delivered to the browser. 4. If exploitation is successful, then it will give the adversary code execution on the user's system unless other protections are in place. * In some cases a second visit to the website after the initial scan is required before exploit code is delivered. Unlike [Exploit Public-Facing Application](https://attack.mitre.org/techniques/T1190), the focus of this technique is to exploit software on a client endpoint upon visiting a website. This will commonly give an adversary access to systems on the internal network instead of external systems that may be in a DMZ. Adversaries may also use compromised websites to deliver a user to a malicious application designed to [Steal Application Access Token](https://attack.mitre.org/techniques/T1528)s, like OAuth tokens, to gain access to protected applications and information. These malicious applications have been delivered through popups on legitimate websites.(Citation: Volexity OceanLotus Nov 2017)

Name
T1197

ID
T1197

Description

Adversaries may abuse BITS jobs to persistently execute code and perform various background tasks. Windows Background Intelligent Transfer Service (BITS) is a low-bandwidth, asynchronous file transfer mechanism exposed through [Component Object Model](https://attack.mitre.org/techniques/T1559/001) (COM).(Citation: Microsoft COM) (Citation: Microsoft BITS) BITS is commonly used by updaters, messengers, and other applications preferred to operate in the background (using available idle bandwidth) without interrupting other networked applications. File transfer tasks are implemented as BITS jobs, which contain a queue of one or more file operations. The interface to create and manage BITS jobs is accessible through [PowerShell](https://attack.mitre.org/techniques/T1059/001) and the [BITSAdmin](https://attack.mitre.org/software/S0190) tool. (Citation: Microsoft BITS)(Citation: Microsoft BITSAdmin) Adversaries may abuse BITS to download (e.g. [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105)), execute, and even clean up after running malicious code (e.g. [Indicator Removal](https://attack.mitre.org/techniques/T1070)). BITS tasks are self-contained in the BITS job database, without new files or registry modifications, and often permitted by host firewalls.(Citation: CTU BITS Malware June 2016)(Citation: Mondok Windows PiggyBack BITS May 2007)(Citation: Symantec BITS May 2007) BITS enabled execution may also enable persistence by creating long-standing jobs (the default maximum lifetime is 90 days and extendable) or invoking an arbitrary program when a job completes or errors (including after system reboots). (Citation: PaloAlto UBoatRAT Nov 2017)(Citation: CTU BITS Malware June 2016) BITS upload functionalities can also be used to perform [Exfiltration Over Alternative Protocol](https://attack.mitre.org/techniques/T1048).(Citation: CTU BITS Malware June 2016)

Name

T1574

ID

T1574

Description

Adversaries may execute their own malicious payloads by hijacking the way operating systems run programs. Hijacking execution flow can be for the purposes of persistence, since this hijacked execution may reoccur over time. Adversaries may also use these mechanisms to elevate privileges or evade defenses, such as application control or other restrictions on execution. There are many ways an adversary may hijack the flow of

execution, including by manipulating how the operating system locates programs to be executed. How the operating system locates libraries to be used by a program can also be intercepted. Locations where the operating system looks for programs/resources, such as file directories and in the case of Windows the Registry, could also be poisoned to include malicious payloads.

Name

T1064

ID

T1064

Description

This technique has been deprecated. Please use [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059) where appropriate. Adversaries may use scripts to aid in operations and perform multiple actions that would otherwise be manual. Scripting is useful for speeding up operational tasks and reducing the time required to gain access to critical resources. Some scripting languages may be used to bypass process monitoring mechanisms by directly interacting with the operating system at an API level instead of calling other programs. Common scripting languages for Windows include VBScript and [PowerShell](https://attack.mitre.org/techniques/T1086) but could also be in the form of command-line batch scripts. Scripts can be embedded inside Office documents as macros that can be set to execute when files used in [Spearphishing Attachment](https://attack.mitre.org/techniques/T1193) and other types of spearphishing are opened. Malicious embedded macros are an alternative means of execution than software exploitation through [Exploitation for Client Execution](https://attack.mitre.org/techniques/T1203), where adversaries will rely on macros being allowed or that the user will accept to activate them. Many popular offensive frameworks exist which use forms of scripting for security testers and adversaries alike. Metasploit (Citation: Metasploit_Ref), Veil (Citation: Veil_Ref), and PowerSploit (Citation: Powersploit) are three examples that are popular among penetration testers for exploit and post-compromise operations and include many features for evading defenses. Some adversaries are known to use PowerShell. (Citation: Alperovitch 2014)

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

T1105

ID

T1105

Description

Adversaries may transfer tools or other files from an external system into a compromised environment. Tools or files may be copied from an external adversary-controlled system to the victim network through the command and control channel or through alternate protocols such as [ftp](https://attack.mitre.org/software/S0095). Once present, adversaries may also transfer/spread tools between victim devices within a compromised environment (i.e. [Lateral Tool Transfer](https://attack.mitre.org/techniques/T1570)). On Windows, adversaries may use various utilities to download tools, such as `copy`, `finger`, [certutil](https://attack.mitre.org/software/S0160), and [PowerShell](https://attack.mitre.org/

techniques/T1059/001) commands such as `IEX(New-Object Net.WebClient).downloadString()` and `Invoke-WebRequest`. On Linux and macOS systems, a variety of utilities also exist, such as `curl`, `scp`, `sftp`, `tftp`, `rsync`, `finger`, and `wget`. (Citation: t1105_lolbas) Adversaries may also abuse installers and package managers, such as `yum` or `winget`, to download tools to victim hosts. Files can also be transferred using various [Web Service](https://attack.mitre.org/techniques/T1102)s as well as native or otherwise present tools on the victim system.(Citation: PTSecurity Cobalt Dec 2016) In some cases, adversaries may be able to leverage services that sync between a web-based and an on-premises client, such as Dropbox or OneDrive, to transfer files onto victim systems. For example, by compromising a cloud account and logging into the service's web portal, an adversary may be able to trigger an automatic syncing process that transfers the file onto the victim's machine.(Citation: Dropbox Malware Sync)

Name

T1204

ID

T1204

Description

An adversary may rely upon specific actions by a user in order to gain execution. Users may be subjected to social engineering to get them to execute malicious code by, for example, opening a malicious document file or link. These user actions will typically be observed as follow-on behavior from forms of [Phishing](https://attack.mitre.org/techniques/T1566). While [User Execution](https://attack.mitre.org/techniques/T1204) frequently occurs shortly after Initial Access it may occur at other phases of an intrusion, such as when an adversary places a file in a shared directory or on a user's desktop hoping that a user will click on it. This activity may also be seen shortly after [Internal Spearphishing](https://attack.mitre.org/techniques/T1534). Adversaries may also deceive users into performing actions such as enabling [Remote Access Software](https://attack.mitre.org/techniques/T1219), allowing direct control of the system to the adversary, or downloading and executing malware for [User Execution](https://attack.mitre.org/techniques/T1204). For example, tech support scams can be facilitated through [Phishing](https://attack.mitre.org/techniques/T1566), vishing, or various forms of user interaction. Adversaries can use a combination of these methods, such as spoofing and promoting toll-free numbers or call centers that are used to direct victims to malicious websites, to

deliver and execute payloads containing malware or [Remote Access Software](https://attack.mitre.org/techniques/T1219).(Citation: Telephone Attack Delivery)

Name

T1036

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) Masquerading may also include the use of [Proxy](https://attack.mitre.org/techniques/T1090) or VPNs to disguise IP addresses, which can allow adversaries to blend in with normal network traffic and bypass conditional access policies or anti-abuse protections.

Name

T1195

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

T1053

ID

T1053

Description

Adversaries may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code. Utilities exist within all major operating systems to schedule programs or scripts to be executed at a specified date and time. A task can also be scheduled on a remote system, provided the proper authentication is met (ex: RPC and file and printer sharing in Windows environments). Scheduling a task on a remote system typically may require being a member of an admin or otherwise privileged group on the remote system.(Citation: TechNet Task Scheduler Security) Adversaries may use task scheduling to execute programs at system startup or on a scheduled basis for persistence. These mechanisms can also be abused to run a process under the context of a specified account (such as one with elevated permissions/privileges). Similar to [System Binary Proxy Execution](https://attack.mitre.org/techniques/T1218), adversaries have also abused task scheduling to potentially mask one-time execution under a trusted system process. (Citation: ProofPoint Serpent)

Intrusion-Set

Name
PikaBot

Malware

Name
QakBot - S0650
Name
PikaBot
Name
DarkGate
Name
QBot
Description
[QakBot](https://attack.mitre.org/software/S0650) is a modular banking trojan that has been used primarily by financially-motivated actors since at least 2007. [QakBot](https://attack.mitre.org/software/S0650) is continuously maintained and developed and has evolved from an information stealer into a delivery agent for ransomware, most notably [ProLock](https://attack.mitre.org/software/S0654) and [Egregor](https://attack.mitre.org/software/S0554).(Citation: Trend Micro Qakbot December 2020)(Citation: Red Canary Qbot)(Citation: Kaspersky QakBot September 2021)(Citation: ATT QakBot April 2021)

Url

Value
http://newssocialwork.com/public/FNFY.zip
http://86.38.225.106:2221
http://57.128.165.176:1372
http://204.44.125.68/mcqef/yPXpC.xn--txt-to0a.
http://178.18.246.136:2078
http://103.124.105.147/KNaDVX/0.2642713404338389.dat
http://103.124.105.147/KNaDVX/.xn--dat-9o0a

IPv4-Addr

Value
86.38.225.106
85.195.115.20
57.128.165.176
204.44.125.68
178.18.246.136
103.124.105.147

StixFile

Value
f3f1492d65b8422125846728b320681baa05a6928fbbd25b16fa28b352b1b512
d26ab01b293b2d439a20d1dffc02a5c9f2523446d811192836e26d370a34d1b4
d4bc0db353dd0051792dd1bfd5a286d3f40d735e21554802978a97599205bd04
bcd3321b03c2cba73bddca46c8a509096083e428b81e88ed90b0b7d4bd3ba4f5
aab0e74b9c6f1326d7ecea9a0de137c76d52914103763ac6751940693f26cbb1
9fc72bdf215a1ff8c22354aac4ad3c19b98a115e448cb60e1b9d3948af580c82
9a4b89276c65d7f17c9568db5e5744ed94244be7ab222bedd8b64f25695ef849
89dc50024836f9ad406504a3b7445d284e97ec5dafdd8f2741f496cac84ccda9
800fa26f895d65041ddf12c421b73eea7f452d32753f4972b05e6b12821c863a
7b1c5147c903892f8888f91c98097c89e419ddcc89958a33e294e6dd192b6d4e
4c29552b5fcd20e5ed8ec72dd345f2ea573e65412b65c99d897761d97c35ebfd
49d8fb17458ca0e9eaff8e3b9f059a9f9cf474cc89190ba42ff4f1e683e09b72

External References

- https://www.mcafee.com/blogs/other-blogs/mcafee-labs/distinctive-campaign-evolution-of-pikabot-malware/
- https://otx.alienvault.com/pulse/660fc68bc14abeb7daf23d42