Sep 25 2023

NETMANAGEIT

Intelligence Report

Cyberespionage Attacks Against Southeast Asian Government Linked to Stately Taurus, Aka Mustang Panda

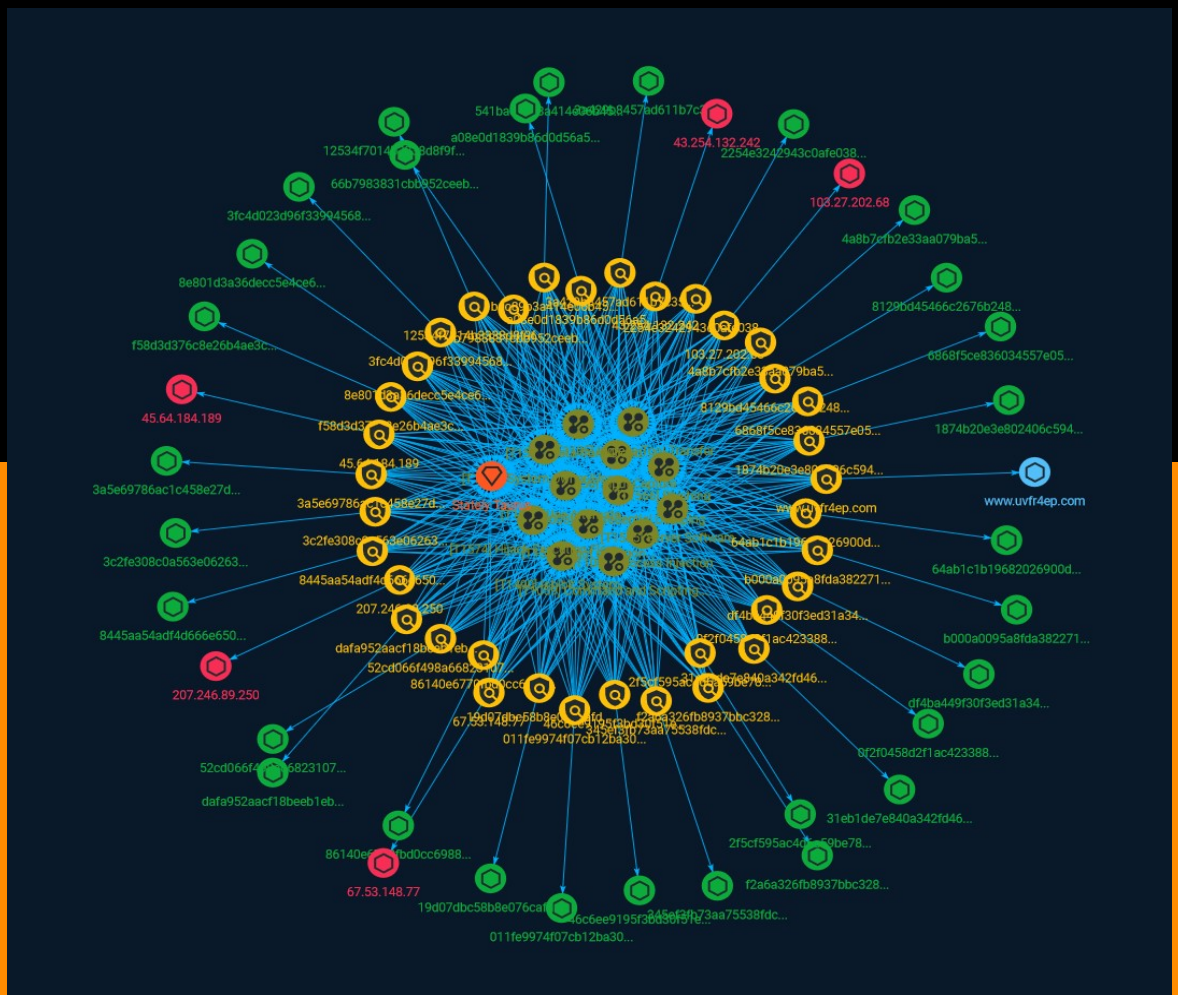

Table of contents

Overview

Entities

Observables

External References

Overview

Description

An advanced persistent threat (APT) group suspected with moderate-high confidence to be Stately Taurus engaged in a number of cyberespionage intrusions targeting a government in Southeast Asia. The intrusions took place from at least the second quarter of 2021 to the third quarter of 2023. Based on our observations and analysis, the attackers gathered and exfiltrated sensitive documents and other types of files from compromised networks.

Confidence

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

15 / 100

Attack-Pattern

Name
OS Credential Dumping
ID
T1003
Description
Adversaries may attempt to dump credentials to obtain account login and credential material, normally in the form of a hash or a clear text password, from the operating system and software. Credentials can then be used to perform [Lateral Movement](https://attack.mitre.org/tactics/TA0008) and access restricted information. Several of the tools mentioned in associated sub-techniques may be used by both adversaries and professional security testers. Additional custom tools likely exist as well.
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

Input Capture

ID

T1056

Description

Adversaries may use methods of capturing user input to obtain credentials or collect information. During normal system usage, users often provide credentials to various different locations, such as login pages/portals or system dialog boxes. Input capture mechanisms may be transparent to the user (e.g. [Credential API Hooking](https://attack.mitre.org/techniques/T1056/004)) or rely on deceiving the user into providing input into what they believe to be a genuine service (e.g. [Web Portal Capture](https://attack.mitre.org/techniques/T1056/003)).

Name

Process Injection

ID

T1055

Description

Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges. Process injection is a method of executing arbitrary code in the address space of a separate live process. Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via process injection may also evade detection from security products since the execution is masked under a legitimate process. There are many different ways to inject code into a process, many of which abuse legitimate functionalities. These implementations exist for every major OS but are typically platform specific. More sophisticated samples may perform multiple process injections to segment modules and further evade detection, utilizing named pipes or other inter-process communication (IPC) mechanisms as a communication channel.

Name

Use Alternate Authentication Material

ID

T1550

Description

Adversaries may use alternate authentication material, such as password hashes, Kerberos tickets, and application access tokens, in order to move laterally within an environment and bypass normal system access controls. Authentication processes generally require a valid identity (e.g., username) along with one or more authentication factors (e.g., password, pin, physical smart card, token generator, etc.). Alternate authentication material is legitimately generated by systems after a user or application successfully authenticates by providing a valid identity and the required authentication factor(s). Alternate authentication material may also be generated during the identity creation process. (Citation: NIST Authentication)(Citation: NIST MFA) Caching alternate authentication material allows the system to verify an identity has successfully authenticated without asking the user to reenter authentication factor(s). Because the alternate authentication must be maintained by the system—either in memory or on disk—it may be at risk of being stolen through [Credential Access](https://attack.mitre.org/tactics/TA0006) techniques. By stealing alternate authentication material, adversaries are able to bypass system access controls and authenticate to systems without knowing the plaintext password or any additional authentication factors.

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

Inhibit System Recovery

ID

T1490

Description

Adversaries may delete or remove built-in data and turn off services designed to aid in the recovery of a corrupted system to prevent recovery.(Citation: Talos Olympic Destroyer 2018) (Citation: FireEye WannaCry 2017) This may deny access to available backups and recovery options. Operating systems may contain features that can help fix corrupted systems, such as a backup catalog, volume shadow copies, and automatic repair features. Adversaries may disable or delete system recovery features to augment the effects of [Data Destruction](https://attack.mitre.org/techniques/T1485) and [Data Encrypted for Impact] (https://attack.mitre.org/techniques/T1486).(Citation: Talos Olympic Destroyer 2018) (Citation: FireEye WannaCry 2017) Furthermore, adversaries may disable recovery notifications, then corrupt backups.(Citation: disable_notif_synology_ransom) A number of native Windows utilities have been used by adversaries to disable or delete system recovery features: * `vssadmin.exe` can be used to delete all volume shadow copies on a system - `vssadmin.exe delete shadows /all /quiet` * [Windows Management Instrumentation](https://attack.mitre.org/techniques/T1047) can be used to delete volume shadow copies - `wmic shadowcopy delete` * `wbadmin.exe` can be used to delete the Windows Backup Catalog - `wbadmin.exe delete catalog -quiet` * `bcdedit.exe` can be used to disable automatic Windows recovery features by modifying boot configuration data - `bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no` * `REAgentC.exe` can be used to disable Windows Recovery Environment (WinRE) repair/recovery options of an infected system On network devices, adversaries may leverage [Disk Wipe](https://attack.mitre.org/techniques/T1561) to delete backup firmware images and reformat the file system, then [System Shutdown/Reboot] (https://attack.mitre.org/techniques/T1529) to reload the device. Together this activity may leave network devices completely inoperable and inhibit recovery operations. Adversaries may also delete “online” backups that are connected to their network – whether via network storage media or through folders that sync to cloud services.(Citation: ZDNet Ransomware Backups 2020) In cloud environments, adversaries may disable versioning and backup policies and delete snapshots, machine images, and prior versions of objects designed to be used in disaster recovery scenarios.(Citation: Dark Reading Code Spaces Cyber Attack)(Citation: Rhino Security Labs AWS S3 Ransomware)

Name

Data from Cloud Storage

ID

T1530

Description

Adversaries may access data from improperly secured cloud storage. Many cloud service providers offer solutions for online data object storage such as Amazon S3, Azure Storage, and Google Cloud Storage. These solutions differ from other storage solutions (such as SQL or Elasticsearch) in that there is no overarching application. Data from these solutions can be retrieved directly using the cloud provider's APIs. In other cases, SaaS application providers such as Slack, Confluence, and Salesforce also provide cloud storage solutions as a peripheral use case of their platform. These cloud objects can be extracted directly from their associated application.(Citation: EA Hacked via Slack - June 2021)(Citation: SecureWorld - How Secure Is Your Slack Channel - Dec 2021)(Citation: HackerNews - 3 SaaS App Cyber Attacks - April 2022)(Citation: Dark Clouds_Usenix_Mulazzani_08_2011) Adversaries may collect sensitive data from these cloud storage solutions. Providers typically offer security guides to help end users configure systems, though misconfigurations are a common problem.(Citation: Amazon S3 Security, 2019)(Citation: Microsoft Azure Storage Security, 2019)(Citation: Google Cloud Storage Best Practices, 2019) There have been numerous incidents where cloud storage has been improperly secured, typically by unintentionally allowing public access to unauthenticated users, overly-broad access by all users, or even access for any anonymous person outside the control of the Identity Access Management system without even needing basic user permissions. This open access may expose various types of sensitive data, such as credit cards, personally identifiable information, or medical records.(Citation: Trend Micro S3 Exposed PII, 2017) (Citation: Wired Magecart S3 Buckets, 2019)(Citation: HIPAA Journal S3 Breach, 2017) (Citation: Rclone-mega-extortion_05_2021) Adversaries may also obtain then abuse leaked credentials from source repositories, logs, or other means as a way to gain access to cloud storage objects.

Name

Server Software Component

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

Hijack Execution Flow

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

Ingress Tool Transfer

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)). 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) 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)

Name

Command and Scripting Interpreter

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

System Owner/User Discovery

ID

T1033

Description

Adversaries may attempt to identify the primary user, currently logged in user, set of users that commonly uses a system, or whether a user is actively using the system. They may do this, for example, by retrieving account usernames or by using [OS Credential Dumping](https://attack.mitre.org/techniques/T1003). The information may be collected in a number of different ways using other Discovery techniques, because user and username details are prevalent throughout a system and include running process ownership, file/directory ownership, session information, and system logs. Adversaries may use the information from [System Owner/User Discovery](https://attack.mitre.org/techniques/T1033) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Various utilities and commands may acquire this information, including `whoami`. In macOS and Linux, the currently logged in user can be identified with `w` and `who`. On macOS the `dscl . list /Users | grep -v '_'` command can also be used to enumerate user accounts. Environment variables, such as `%USERNAME%` and `$USER`, may also be used to access this information. On network devices, [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) commands such as `show users` and `show ssh` can be used to display users currently logged into the device.(Citation: show_ssh_users_cmd_cisco)(Citation: US-CERT TA18-106A Network Infrastructure Devices 2018)

Indicator

Name

207.246.89.250

Description

ISP: The Constant Company, LLC **OS:** Windows Server 2019 (version 1809) (build 10.0.17763) ---------- Hostnames: - 207.246.89.250.vultrusercontent.com ---------- Domains: - vultrusercontent.com ---------- 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 1809)/Windows Server 2019 (version 1809) OS Build: 10.0.17763 Target Name: VULTR-GUEST NetBIOS Domain Name: VULTR-GUEST NetBIOS Computer Name: VULTR-GUEST DNS Domain Name: vultr-guest FQDN: vultr-guest ``` ---------- **5985:** ``` HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Sat, 23 Sep 2023 15:35:26 GMT Connection: close Content-Length: 315 WinRM NTLM Info: OS: Windows Server 2019 (version 1809) OS Build: 10.0.17763 Target Name: VULTR-GUEST NetBIOS Domain Name: VULTR-GUEST NetBIOS Computer Name: VULTR-GUEST DNS Domain Name: vultr-guest FQDN: vultr-guest ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '207.246.89.250']

Name

8129bd45466c2676b248c08bb0efcd9ccc8b684abf3435e290fcf4739c0a439f

Description

Win32:Evo-gen\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8129bd45466c2676b248c08bb0efcd9ccc8b684abf3435e290fcf4739c0a439f']

Name

f2a6a326fb8937bbc32868965f7475f4af0f42f3792e80156cc57108fc09c034

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f2a6a326fb8937bbc32868965f7475f4af0f42f3792e80156cc57108fc09c034']

Name

f58d3d376c8e26b4ae3c2bbaa4ae76ca183f32823276e6432a945bcbc63266d9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f58d3d376c8e26b4ae3c2bbaa4ae76ca183f32823276e6432a945bcbc63266d9']

Name

1874b20e3e802406c594341699c5863a2c07c4c79cf762888ee28142af83547f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1874b20e3e802406c594341699c5863a2c07c4c79cf762888ee28142af83547f']

Name

67.53.148.77

Description

ISP: Charter Communications Inc **OS:** None ---------- Hostnames: - rrcs-67-53-148-77.west.biz.rr.com ---------- Domains: - rr.com ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.4p1 Raspbian-5+deb11u1 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDj3ElixiEArGgIgOLONlKVh1cTbwMgIs5mDZY/usNnpkoG Rl4VCUY10iElP7EnH0ZslgAA8OHlPCt+CJ96/n6Gyadm/5o17meEYe0ibRWXfLxHdvHOYNBVi8lE L8xkfDtRGym00VnZBhrMCwDlBQDDEiNsOsAMF38SNJHGusnOeD1Ya+5cdoexC4BX8vcy9DV0Ht VV RTEcQ6b025M7LO6eEAZNy/2+j19VF4UTpMD/ 4w3eSl2vgs96OSZpoMN5MTZmX840KqFyZOXw7K82 ZT/0u9DfNMq2EJKX6iBGEEax/ rt+sg0oj2Tb/HZ9lXt3YlV1KzFJYr+OOYKj57fYk2jt Fingerprint: f8:dd:f8:55:75:df:3d:49:78:6a:ff: 84:04:c5:63:48 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 Server: nginx Date: Mon, 25 Sep 2023 06:47:07 GMT Content-Type: application/octet-stream Content-Length: 1552 Last-Modified: Tue, 02 Feb 2021 23:45:54 GMT ETag: "6019e432-610" X-Varnish: 3573057 Age: 0 Via: 1.1 varnish (Varnish/6.5) Accept-Ranges: bytes Connection: keep-alive ``` ---------- **443:** ``` HTTP/1.1 200 OK Server: nginx Date: Sun, 24 Sep 2023 22:02:18 GMT Content-Type: application/octet-stream Content-Length: 1552 Last-Modified: Tue, 02 Feb 2021 23:45:54 GMT Connection: keep-alive ETag: "6019e432-610" Accept-Ranges: bytes ``` HEARTBLEED: 2023/09/24 22:02:31 67.53.148.77:443 - SAFE ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '67.53.148.77']

Name

66b7983831cbb952ceeb1ffff608880f1805f1df0b062cef4c17b258b7f478ce

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '66b7983831cbb952ceeb1ffff608880f1805f1df0b062cef4c17b258b7f478ce']

Name

0f2f0458d2f1ac4233883e96fe1f4cc6db1551cdcfdd49c43311429af03a1cd5

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0f2f0458d2f1ac4233883e96fe1f4cc6db1551cdcfdd49c43311429af03a1cd5']

Name

3c2fe308c0a563e06263bbacf793bbe9b2259d795fcc36b953793a7e499e7f71

Description

SHA256 of 23873bf2670cf64c2440058130548d4e4da412dd SHA256 of 23873bf2670cf64c2440058130548d4e4da412dd

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3c2fe308c0a563e06263bbacf793bbe9b2259d795fcc36b953793a7e499e7f71']

Name

103.27.202.68

Description

ISP: Bangmod Enterprise Co., Ltd. **OS:** Ubuntu ---------- Hostnames: - 103-27-202-68.static.bangmod-idc.com ---------- Domains: - bangmod-idc.com ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.2p1 Ubuntu-4 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQCnKsmUZrpGHMOkEImu7/61sI4wbylvwZPEA+w29hVOn HSx DfboH5rcWxSIkJW0RV/ cU6Ee9qqgjUQha0a+sMymy43sA6poz0FhNCw47BQhys5YeC23hBxAnx2p / TTz4O+h9EIb4K3UlUqxOSso0Am+MQddf76beRRda0+pY0vc8Ub5xWdIxwtI9nflI0lnZiT0n7yn Vx9tqrtYcsixndDyeo48cNqjtPdmxuiXej7sZbiltx+sYUeIKLwpjIyLFAAJtwlBk7qYfxcrvySH W01VV9riR+n20m9wn3bYQhuLue22nsGvagnPMZAhhIIqeUf0GVopzYa37UtmFRHJk5zt Fingerprint: 51:c5:b3:cb:7f:2c:f9:22:49:5c:38:23:32:57:71:05 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 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '103.27.202.68']

Name

46c6ee9195f3bd30f51eb6611623aad1ba17f5e0cde0b5523ab51e0c5b641dbf

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '46c6ee9195f3bd30f51eb6611623aad1ba17f5e0cde0b5523ab51e0c5b641dbf']

Name

3fc4d023d96f339945683f6dc7d9e19a9a62b901bef6dc26c5918ce9508be273

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3fc4d023d96f339945683f6dc7d9e19a9a62b901bef6dc26c5918ce9508be273']

Name

64ab1c1b19682026900d060b969ab3c3ab860988733b7e7bf3ba78a4ea0340b9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '64ab1c1b19682026900d060b969ab3c3ab860988733b7e7bf3ba78a4ea0340b9']

Name

86140e6770fbd0cc6988f025d52bb4f59c0d78213c75451b42c9f812fe1a9354

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '86140e6770fbd0cc6988f025d52bb4f59c0d78213c75451b42c9f812fe1a9354']

Name

43.254.132.242

Description

CC=TH ASN=AS131447 POPIDC powered by CSLoxinfo

Pattern Type

stix

Pattern

[ipv4-addr:value = '43.254.132.242']

Name

2f5cf595ac4d6a59be78a781c5ba126c2ff6d6e5956dc0a7602e6ba8e6665694

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2f5cf595ac4d6a59be78a781c5ba126c2ff6d6e5956dc0a7602e6ba8e6665694']

Name

45.64.184.189

Description

ISP: Bangmod Enterprise Co., Ltd. **OS:** Ubuntu ---------- Hostnames: - 45-64-184-189.static.bangmod-idc.com ---------- Domains: - bangmod-idc.com ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.2p1 Ubuntu-4 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDeR3++VXLxFHq37/ yqa7DP4VJVBsJEA5dNDkXDE+I03kXO 1vlxp/nzyyJX667ZnS0hB/sTf/ 5tfcXbafCPpT9o61u2Sz2zLknmb0zbW2yhShVMTUp5RA0U6AOg Hak5yKvkXrNZjUJpc+F+jwewIOo8GS3QTv0vNWfgPo+GmezpJxeHLw6bNblcWFvv+qq22Y51ixJr TRMX9p9B15gTnZ44uFGxHwUboLwxSdIgCX+yLeW1d5sZtYErL4e1WjpER+N8vlqzNiL2JZG27C23 ngv6Ngxsvu7SVCa7hqJ7UBnM9p2ZmmbOPIImAm76AIbzuKzTj91MDIBz5dGNlM67oBHT Fingerprint: 25:da:35:21:ec:a6:3e:f4:0d:c7:40:4a:17:5a:d9:2b 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 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.64.184.189']

Name

6868f5ce836034557e05c7ddea006a91d6fc59de7e235c9b08787bd6dbd2b837

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6868f5ce836034557e05c7ddea006a91d6fc59de7e235c9b08787bd6dbd2b837']

Name

19d07dbc58b8e076cafd98c25cae5d7ac6f007db1c8ec0fae4ce6c7254b8f073

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '19d07dbc58b8e076cafd98c25cae5d7ac6f007db1c8ec0fae4ce6c7254b8f073']

Name

541bac89b3a414e06b45d778f86b245675922e8b11f866c8b6a827c5d418e598

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '541bac89b3a414e06b45d778f86b245675922e8b11f866c8b6a827c5d418e598']

Name

df4ba449f30f3ed31a344931dc77233b27e06623355ece23855ee4fe8a75c267

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'df4ba449f30f3ed31a344931dc77233b27e06623355ece23855ee4fe8a75c267']

Name

8445aa54adf4d666e65084909a7b989a190ec6eca2844546c2e99a8cfb832fad

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8445aa54adf4d666e65084909a7b989a190ec6eca2844546c2e99a8cfb832fad']

Name

2254e3242943c0afe038baeafe8381bbff136e6d8f681f0f446bf0e458900643

Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '2254e3242943c0afe038baeafe8381bbff136e6d8f681f0f446bf0e458900643']
Name
345ef3fb73aa75538fdcf780d2136642755a9f20dbd22d93bee26e93fb6ab8fd
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '345ef3fb73aa75538fdcf780d2136642755a9f20dbd22d93bee26e93fb6ab8fd']
Name
8e801d3a36decc5e4ce6fd3e8e45b098966aef8cbe7535ed0a789575775a68b6
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '8e801d3a36decc5e4ce6fd3e8e45b098966aef8cbe7535ed0a789575775a68b6']

Name

www.uvfr4ep.com

Pattern Type

stix

Pattern

[hostname:value = 'www.uvfr4ep.com']

Name

52cd066f498a66823107aed7eaa4635eee6b7914acded926864f1aae59571991

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '52cd066f498a66823107aed7eaa4635eee6b7914acded926864f1aae59571991']

Name

a08e0d1839b86d0d56a52d07123719211a3c3d43a6aa05aa34531a72ed1207dc

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a08e0d1839b86d0d56a52d07123719211a3c3d43a6aa05aa34531a72ed1207dc']

Name

31eb1de7e840a342fd468e558e5ab627bcb4c542a8fe01aec4d5ba01d539a0fc

Description

HackTool:Win32/Mimikatz.D

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '31eb1de7e840a342fd468e558e5ab627bcb4c542a8fe01aec4d5ba01d539a0fc']

Name

3a5e69786ac1c458e27d38a966425abb6fb493a41110393a4878c811557a3b5b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3a5e69786ac1c458e27d38a966425abb6fb493a41110393a4878c811557a3b5b']

Name

4a8b7cfb2e33aa079ba51166591c7a210ad8b3c7c7f242fccf8cb2e71e8e40d5

Description

DotNET_DotFuscator

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4a8b7cfb2e33aa079ba51166591c7a210ad8b3c7c7f242fccf8cb2e71e8e40d5']

Name

011fe9974f07cb12ba30e69e7a84e5cb489ce14a81bced59a11031fc0c3681b7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '011fe9974f07cb12ba30e69e7a84e5cb489ce14a81bced59a11031fc0c3681b7']

Name

12534f7014b3338d8f9f86ff1bbeacf8c80ad03f1d0d19077ff0e406c58b5133

Description

ALF:HSTR:Exploit:Win32/CVE-2020-0796.A

Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '12534f7014b3338d8f9f86ff1bbeacf8c80ad03f1d0d19077ff0e406c58b5133']
Name
b000a0095a8fda38227103f253b6d79134b862a83df50315d7d9c5b537fd994b
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'b000a0095a8fda38227103f253b6d79134b862a83df50315d7d9c5b537fd994b']
Name
dafa952aacf18beeb1ebf47620589639223a2e99fb2fa5ce2de1e7ef7a56caa0
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'dafa952aacf18beeb1ebf47620589639223a2e99fb2fa5ce2de1e7ef7a56caa0']

Name
3a429b8457ad611b7c3528e4b41e8923dd2aee32ccd2cc5cf5ff83e69c1253c2
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '3a429b8457ad611b7c3528e4b41e8923dd2aee32ccd2cc5cf5ff83e69c1253c2']

Intrusion-Set

Name
Stately Taurus

StixFile

Value
8e801d3a36decc5e4ce6fd3e8e45b098966aef8cbe7535ed0a789575775a68b6
011fe9974f07cb12ba30e69e7a84e5cb489ce14a81bced59a11031fc0c3681b7
2254e3242943c0afe038baeafe8381bbff136e6d8f681f0f446bf0e458900643
541bac89b3a414e06b45d778f86b245675922e8b11f866c8b6a827c5d418e598
a08e0d1839b86d0d56a52d07123719211a3c3d43a6aa05aa34531a72ed1207dc
f58d3d376c8e26b4ae3c2bbaa4ae76ca183f32823276e6432a945bcbc63266d9
dafa952aacf18beeb1ebf47620589639223a2e99fb2fa5ce2de1e7ef7a56caa0
1874b20e3e802406c594341699c5863a2c07c4c79cf762888ee28142af83547f
345ef3fb73aa75538fdcf780d2136642755a9f20dbd22d93bee26e93fb6ab8fd
46c6ee9195f3bd30f51eb6611623aad1ba17f5e0cde0b5523ab51e0c5b641dbf
31eb1de7e840a342fd468e558e5ab627bcb4c542a8fe01aec4d5ba01d539a0fc
6868f5ce836034557e05c7ddea006a91d6fc59de7e235c9b08787bd6dbd2b837
66b7983831cbb952ceeb1ffff608880f1805f1df0b062cef4c17b258b7f478ce

19d07dbc58b8e076cafd98c25cae5d7ac6f007db1c8ec0fae4ce6c7254b8f073

0f2f0458d2f1ac4233883e96fe1f4cc6db1551cdcfdd49c43311429af03a1cd5

3c2fe308c0a563e06263bbacf793bbe9b2259d795fcc36b953793a7e499e7f71

f2a6a326fb8937bbc32868965f7475f4af0f42f3792e80156cc57108fc09c034

64ab1c1b19682026900d060b969ab3c3ab860988733b7e7bf3ba78a4ea0340b9

12534f7014b3338d8f9f86ff1bbeacf8c80ad03f1d0d19077ff0e406c58b5133

df4ba449f30f3ed31a344931dc77233b27e06623355ece23855ee4fe8a75c267

3fc4d023d96f339945683f6dc7d9e19a9a62b901bef6dc26c5918ce9508be273

b000a0095a8fda38227103f253b6d79134b862a83df50315d7d9c5b537fd994b

4a8b7cfb2e33aa079ba51166591c7a210ad8b3c7c7f242fccf8cb2e71e8e40d5

3a5e69786ac1c458e27d38a966425abb6fb493a41110393a4878c811557a3b5b

86140e6770fbd0cc6988f025d52bb4f59c0d78213c75451b42c9f812fe1a9354

52cd066f498a66823107aed7eaa4635eee6b7914acded926864f1aae59571991

3a429b8457ad611b7c3528e4b41e8923dd2aee32ccd2cc5cf5ff83e69c1253c2

8129bd45466c2676b248c08bb0efcd9ccc8b684abf3435e290fcf4739c0a439f

2f5cf595ac4d6a59be78a781c5ba126c2ff6d6e5956dc0a7602e6ba8e6665694

8445aa54adf4d666e65084909a7b989a190ec6eca2844546c2e99a8cfb832fad

Hostname

Value
www.uvfr4ep.com

IPv4-Addr

Value
103.27.202.68
45.64.184.189
207.246.89.250
43.254.132.242
67.53.148.77

External References

- https://otx.alienvault.com/pulse/6511d6fd63ecbfd938c3580f
- https://unit42.paloaltonetworks.com/stately-taurus-attacks-se-asian-government/