Mar 26 2024

NETMANAGEIT

Intelligence Report

The ghost of TellYouThePass lingers

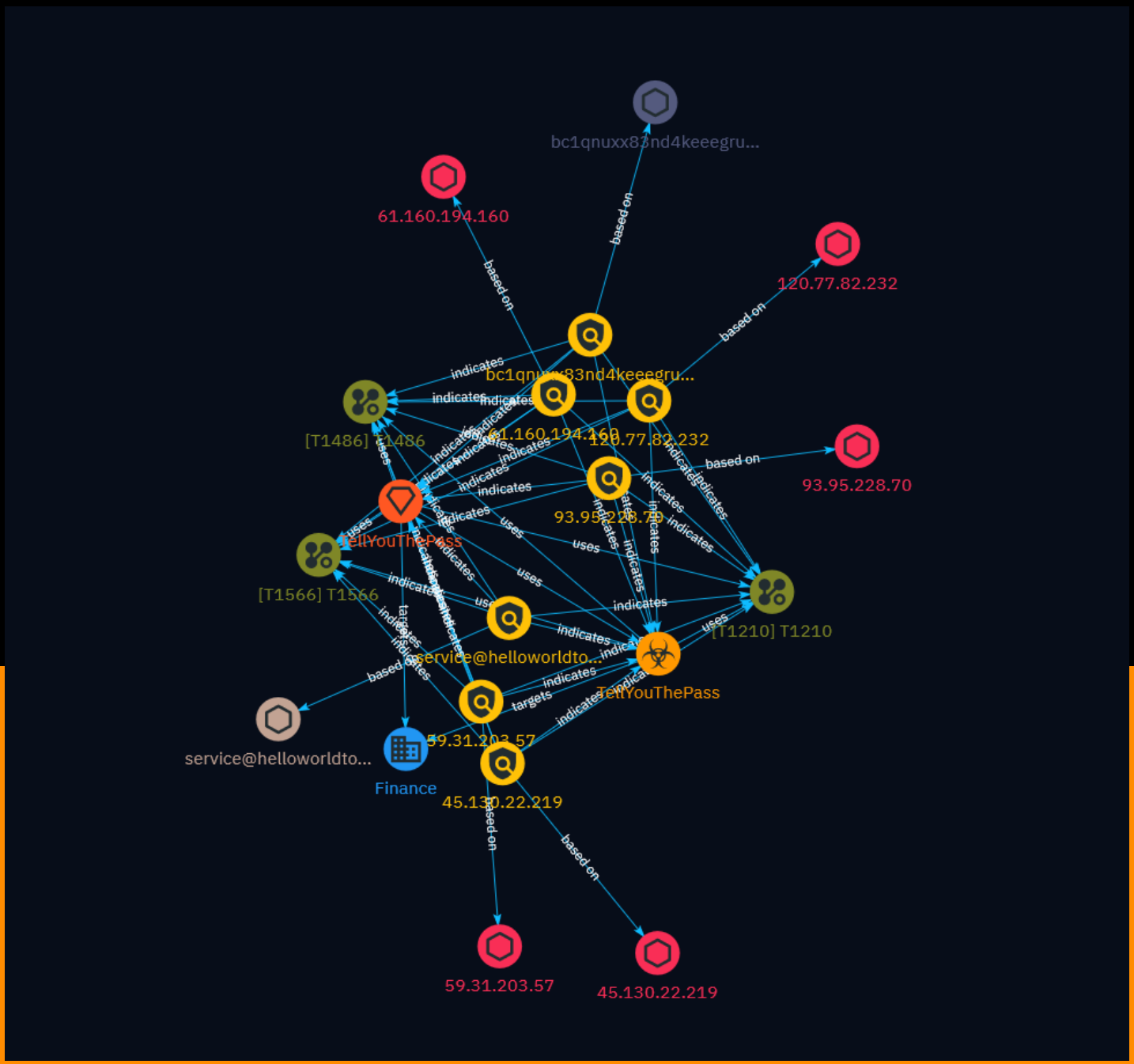

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Recently, 360 Ransomware Service received feedback from many victims from the financial sector that ransomware was implanted in their devices. After analysis, the source of this wave of attacks was successfully identified as the TellYouThePass ransomware family - an old ransomware family specializing in large-scale attacks exploiting server vulnerabilities. The family has already launched 3 larger-scale attacks in 2023, and began wreaking havoc again in early 2024.

Confidence

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

100 / 100

Content

N/A

Indicator

Name
120.77.82.232
Description
ISP: Hangzhou Alibaba Advertising Co.,Ltd. **OS:** - ---------- Services: **8080:** ``` HTTP/1.0 200 OK Server: SimpleHTTP/0.6 Python/3.9.2 Date: Thu, 14 Mar 2024 10:30:41 GMT Content-type: text/html; charset=utf-8 Content-Length: 358 ``` ----------
Pattern Type
stix
Pattern
[ipv4-addr:value = '120.77.82.232']
Name
59.31.203.57
Description
ISP: Korea Telecom **OS:** - ---------- Services: **80:** ``` HTTP/1.1 200 OK Date: Thu, 21 Mar 2024 17:43:37 GMT Transfer-Encoding: chunked Content-Type: text/html; charset=EUC-KR Set-Cookie: JSESSIONID=amBiHHvo77jBJMzREPQCSudYfLT2_2cMtLEy6Do3oRMQBZ9PeUcO!532237831; path=/; HttpOnly Content-Language: ko-KR ``` ---------- **443:** ``` HTTP/1.1 200 OK

Date: Sun, 24 Mar 2024 23:15:18 GMT Transfer-Encoding: chunked Content-Type: text/html; charset=EUC-KR Set-Cookie: JSESSIONID=HBJyvzr0l4-uaEZ247FzE1WbmGWXmvkdixDxISNtytpYHi8ak4WN!532237831; path=/; HttpOnly Content-Language: ko-KR ``` HEARTBLEED: 2024/03/24 23:15:35 59.31.203.57:443 - ERROR: heartbleed: timeout ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '59.31.203.57']

Name

61.160.194.160

Description

ISP: CHINANET-BACKBONE **OS:** Windows Server 2016 (version 1607) (build 10.0.14393) ---------- Services: **443:** ``` HTTP/1.1 403 Forbidden Date: Sat, 9 Mar 2024 14:34:35 GMT Connection: close Content-Security-Policy: block-all-mixed-content Content-Type: text/plain; charset=utf-8 Strict-Transport-Security: max-age=31536000 X-Content-Type-Options: nosniff X-Frame-Options: DENY X-XSS-Protection: 1 Content-Length: 0 ``` HEARTBLEED: 2024/03/09 14:38:10 61.160.194.160:443 - ERROR: heartbleed: timeout ---------- **902:** ``` 220 VMware Authentication Daemon Version 1.10: SSL Required, ServerDaemonProtocol:SOAP, MKSDisplayProtocol:VNC , , NFCSSL supported/t ``` ---------- **3306:** ``` MySQL: Error Message: Host '224.128.71.68' is not allowed to connect to this MySQL server Error Code: 1130 ``` ---------- **5985:** ``` HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Fri, 22 Mar 2024 10:16:59 GMT Connection: close Content-Length: 315 WinRM NTLM Info: OS: Windows Server 2016 (version 1607) OS Build: 10.0.14393 Target Name: IDC-20231003ISP NetBIOS Domain Name: IDC-20231003ISP NetBIOS Computer Name: IDC-20231003ISP DNS Domain Name: IDC-20231003ISP FQDN: IDC-20231003ISP ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '61.160.194.160']

Name

93.95.228.70

Description

ISP: 1984 ehf **OS:** - ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.6 Key type: ssh-ed25519 Key: AAAAC3NzaC1lZDI1NTE5AAAAILapgwprietHToh4gimPJcWZfmZgIAfIOUVmqnic/epa Fingerprint: bb:ef:bb:b2:75:6e:50:78:f2:15:c6:26:39:ab:ce:6a Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 sntrup761x25519-sha512@openssh.com diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 kex-strict-s-v00@openssh.com Server Host Key Algorithms: 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: Fri, 15 Mar 2024 17:26:47 GMT Server: Apache/2.4.52 (Ubuntu) Last-Modified: Thu, 22 Feb 2024 06:05:41 GMT ETag: "29af-611f23baf23cd" Accept-Ranges: bytes Content-Length: 10671 Vary: Accept-Encoding Content-Type: text/html ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '93.95.228.70']

Name

service@helloworldtom.online

Pattern Type

stix

Pattern

[email-addr:value = 'service@helloworldtom.online']

Name

bc1qnuxx83nd4keeegrumtnu8kup8g02yzgff6z53l

Pattern Type

stix

Pattern

[cryptocurrency-wallet:value = 'bc1qnuxx83nd4keeegrumtnu8kup8g02yzgff6z53l']

Name

45.130.22.219

Description

ISP: Owl Limited **OS:** - ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.6 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBKzQ+9ADktGEpzVKLB3b16xM yewZkva7ZRya62CHUmsTYeVvr3oRF5V49JHxB4gGdAJvHDLFNuEPDCd4hw202rw= Fingerprint: 89:36:ea:e7:d8:ab:ba:2a:9d:a1:50:f0:d9:c3:b5:43 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521

sntrup761x25519-sha512@openssh.com diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 kex-strict-s-v00@openssh.com Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 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 Set-Cookie: JSESSIONID=C6CC80429AB46A1A994EA89239F3AA26; Path=/; HttpOnly Content-Type: text/html;charset=ISO-8859-1 Content-Length: 16 Date: Thu, 01 Feb 2024 03:57:16 GMT ``` ---------- **443:** ``` HTTP/1.1 200 Set-Cookie: JSESSIONID=A84AB67650AFD23C335F0B147EB0B669; Path=/; Secure; HttpOnly Content-Type: text/html;charset=ISO-8859-1 Content-Length: 16 Date: Sun, 04 Feb 2024 09:48:54 GMT ``` HEARTBLEED: 2024/02/04 09:48:58 45.130.22.219:443 - SAFE ---------- **465:** ``` ``` ---------- **995:** ``` ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.130.22.219']

Malware

Name
TellYouThePass

Intrusion-Set

Name
TellYouThePass

Attack-Pattern

Name
T1486
ID
T1486
Description
Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources. They can attempt to render stored data inaccessible by encrypting files or data on local and remote drives and withholding access to a decryption key. This may be done in order to extract monetary compensation from a victim in exchange for decryption or a decryption key (ransomware) or to render data permanently inaccessible in cases where the key is not saved or transmitted.(Citation: US-CERT Ransomware 2016)(Citation: FireEye WannaCry 2017)(Citation: US-CERT NotPetya 2017)(Citation: US-CERT SamSam 2018) In the case of ransomware, it is typical that common user files like Office documents, PDFs, images, videos, audio, text, and source code files will be encrypted (and often renamed and/or tagged with specific file markers). Adversaries may need to first employ other behaviors, such as [File and Directory Permissions Modification](https://attack.mitre.org/techniques/T1222) or [System Shutdown/Reboot](https://attack.mitre.org/techniques/T1529), in order to unlock and/or gain access to manipulate these files.(Citation: CarbonBlack Conti July 2020) In some cases, adversaries may encrypt critical system files, disk partitions, and the MBR.(Citation: US-CERT NotPetya 2017) To maximize impact on the target organization, malware designed for encrypting data may have worm-like features to propagate across a network by leveraging other attack techniques like [Valid Accounts](https://attack.mitre.org/techniques/T1078), [OS Credential Dumping](https://attack.mitre.org/techniques/T1003), and [SMB/Windows Admin Shares](https://attack.mitre.org/techniques/T1021/002).(Citation: FireEye WannaCry 2017)(Citation: US-CERT NotPetya 2017) Encryption malware may also leverage [Internal

Defacement](https://attack.mitre.org/techniques/T1491/001), such as changing victim wallpapers, or otherwise intimidate victims by sending ransom notes or other messages to connected printers (known as "print bombing").(Citation: NHS Digital Egregor Nov 2020) In cloud environments, storage objects within compromised accounts may also be encrypted. (Citation: Rhino S3 Ransomware Part 1)

Name

T1210

ID

T1210

Description

Adversaries may exploit remote services to gain unauthorized access to internal systems once inside of a network. Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. A common goal for post-compromise exploitation of remote services is for lateral movement to enable access to a remote system. An adversary may need to determine if the remote system is in a vulnerable state, which may be done through [Network Service Discovery](https://attack.mitre.org/techniques/T1046) or other Discovery methods looking for common, vulnerable software that may be deployed in the network, the lack of certain patches that may indicate vulnerabilities, or security software that may be used to detect or contain remote exploitation. Servers are likely a high value target for lateral movement exploitation, but endpoint systems may also be at risk if they provide an advantage or access to additional resources. There are several well-known vulnerabilities that exist in common services such as SMB (Citation: CIS Multiple SMB Vulnerabilities) and RDP (Citation: NVD CVE-2017-0176) as well as applications that may be used within internal networks such as MySQL (Citation: NVD CVE-2016-6662) and web server services.(Citation: NVD CVE-2014-7169) Depending on the permissions level of the vulnerable remote service an adversary may achieve [Exploitation for Privilege Escalation](https://attack.mitre.org/techniques/T1068) as a result of lateral movement exploitation as well.

Name

T1566

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)

Sector

Name
Finance
Description
Public and private entities involved in the allocation of assets and liabilities over space and time.

IPv4-Addr

Value
120.77.82.232
59.31.203.57
61.160.194.160
93.95.228.70
45.130.22.219

Email-Addr

Value
service@helloworldtom.online

Cryptocurrency-Wallet

Value
bc1qnuxx83nd4keeegrumtnu8kup8g02yzgff6z53l

External References

- https://cert.360.cn/report/detail?id=65fceeb4c09f255b91b17f11
- https://otx.alienvault.com/pulse/6602ca1fb3a72911ae9de39a