Mar 05 2024

NETMANAGEIT

Intelligence Report

Unusual Attack Chain Leads to NTLM Data Theft

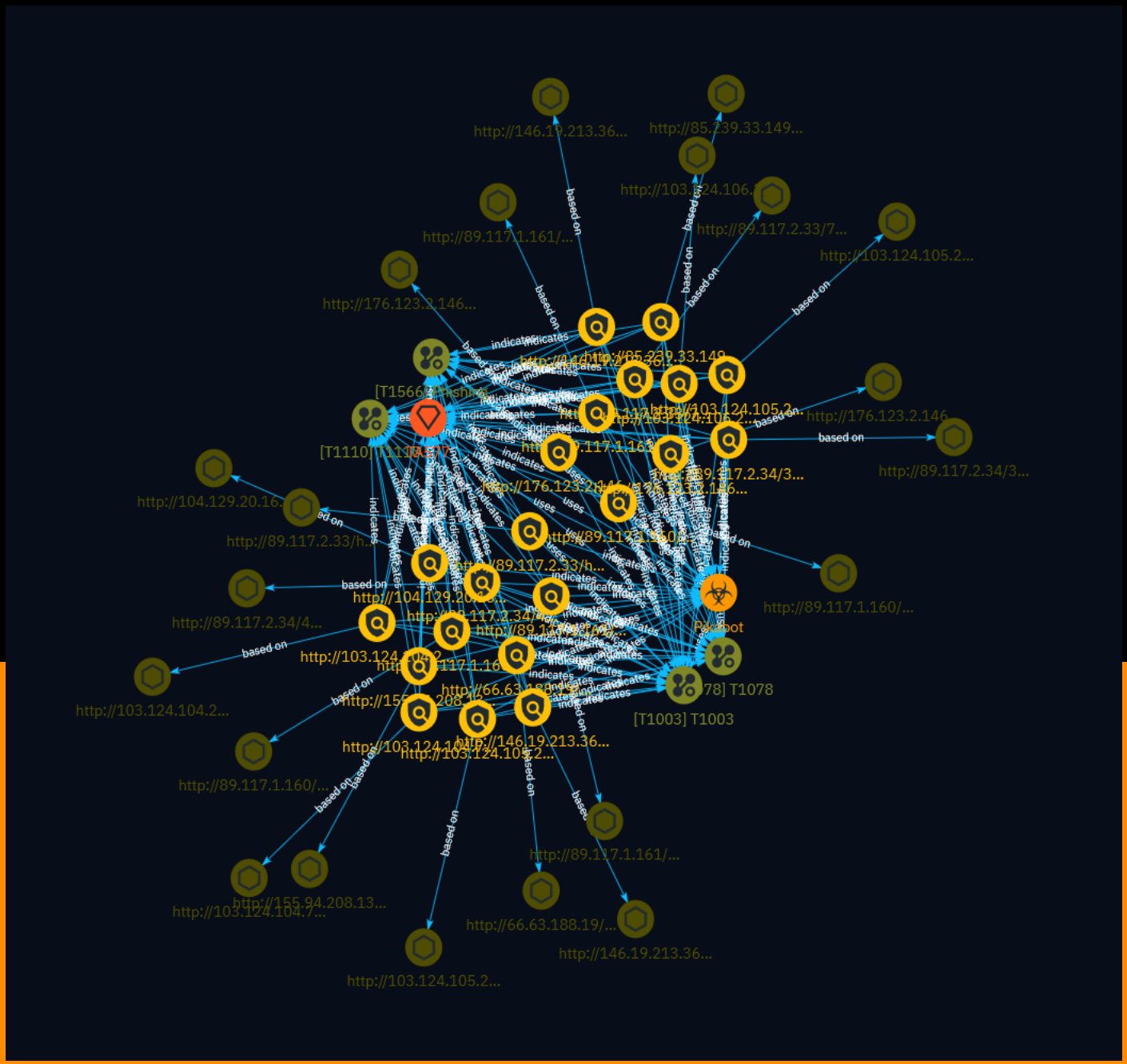

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Proofpoint identified threat actor TA577 using a new attack chain to steal NTLM authentication information for sensitive data gathering and follow-on activity. Campaigns sent tens of thousands of emails with zipped HTML attachments that triggered connections to TA577's SMB servers, potentially compromising NTLM hashes. TA577 has rapidly adopted new tactics recently, suggesting they have resources to iterate delivery methods. Organizations should block outbound SMB to prevent this type of exploitation.

Confidence

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

100 / 100

Content

N/A

Indicator

Name

http://89.117.2.34/4qp/8Y.txt

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:** 89.117.2.34 - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://89.117.2.34/4qp/8Y.txt']

Name

http://89.117.2.34/3m3sxh6/IuM.txt

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:** 89.117.2.34 - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://89.117.2.34/3m3sxh6/IuM.txt']

Name

http://89.117.2.33/hvwsuw/udrh.txt

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:** 89.117.2.33 - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://89.117.2.33/hvwsuw/udrh.txt']

Name

http://89.117.2.33/7ipw/7ohq.txt

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:** 89.117.2.33 - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://89.117.2.33/7ipw/7ohq.txt']

Name

http://89.117.1.161/mtdi/ZQCw.txt

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:** 89.117.1.161 - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://89.117.1.161/mtdi/ZQCw.txt']

Name

http://89.117.1.161/epxq/A.txt

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:** 89.117.1.161 - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://89.117.1.161/epxq/A.txt']

Name

http://89.117.1.160/zkf2r4j/VmD.txt

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:** 89.117.1.160 - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://89.117.1.160/zkf2r4j/VmD.txt']

Name

http://89.117.1.160/4bvt1yw/iC.txt

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:** 89.117.1.160 - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://89.117.1.160/4bvt1yw/iC.txt']

Name

http://85.239.33.149/naams/p3aV.txt

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:** 85.239.33.149 - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://85.239.33.149/naams/p3aV.txt']

Name

http://66.63.188.19/bmkmsw/2.txt

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:** 66.63.188.19 - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://66.63.188.19/bmkmsw/2.txt']

Name

http://176.123.2.146/vbcsn/UOx.txt

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:** 176.123.2.146 - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://176.123.2.146/vbcsn/UOx.txt']

Name

http://176.123.2.146/5aohv/9mn.txt

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:** 176.123.2.146 - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://176.123.2.146/5aohv/9mn.txt']

Name

http://155.94.208.137/tgnd/zH9.txt

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:** 155.94.208.137 - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://155.94.208.137/tgnd/zH9.txt']

Name

http://146.19.213.36/vei/yEZZ.txt

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:** 146.19.213.36 - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://146.19.213.36/vei/yEZZ.txt']

Name

http://146.19.213.36/dbna/H.txt

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:** 146.19.213.36 - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://146.19.213.36/dbna/H.txt']

Name

http://104.129.20.167/xhsmd/bOWEU.txt

Description

- **Unsafe:** False - **Server:** Apache/2.4.41 (Ubu - **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:** 104.129.20.167 - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://104.129.20.167/xhsmd/bOWEU.txt']

Name

http://103.124.106.224/uuny19/bb1nG.txt

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:** 103.124.106.224 - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://103.124.106.224/uuny19/bb1nG.txt']

Name

http://103.124.105.233/yusx/dMA.txt

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:** 103.124.105.233 - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://103.124.105.233/yusx/dMA.txt']

Name

http://103.124.105.208/wha5uxh/D.txt

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:** 103.124.105.208 - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://103.124.105.208/wha5uxh/D.txt']

Name

http://103.124.104.76/wsr6oh/Y.txt

Description

- **Unsafe:** False - **Server:** Apache/2.4.41 (Ubu - **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:** 103.124.104.76 - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://103.124.104.76/wsr6oh/Y.txt']

Name

http://103.124.104.22/zjxb/bO.txt

Description

- **Unsafe:** False - **Server:** Apache/2.4.41 (Ubu - **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:** 103.124.104.22 - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://103.124.104.22/zjxb/bO.txt']

Intrusion-Set

Name
TA577

Malware

Name
Pikabot

Attack-Pattern

Name

T1078

ID

T1078

Description

Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Compromised credentials may be used to bypass access controls placed on various resources on systems within the network and may even be used for persistent access to remote systems and externally available services, such as VPNs, Outlook Web Access, network devices, and remote desktop.(Citation: volexity_0day_sophos_FW) Compromised credentials may also grant an adversary increased privilege to specific systems or access to restricted areas of the network. Adversaries may choose not to use malware or tools in conjunction with the legitimate access those credentials provide to make it harder to detect their presence. In some cases, adversaries may abuse inactive accounts: for example, those belonging to individuals who are no longer part of an organization. Using these accounts may allow the adversary to evade detection, as the original account user will not be present to identify any anomalous activity taking place on their account.(Citation: CISA MFA PrintNightmare) The overlap of permissions for local, domain, and cloud accounts across a network of systems is of concern because the adversary may be able to pivot across accounts and systems to reach a high level of access (i.e., domain or enterprise administrator) to bypass access controls set within the enterprise.(Citation: TechNet Credential Theft)

Name

T1110

ID

T1110

Description

Adversaries may use brute force techniques to gain access to accounts when passwords are unknown or when password hashes are obtained. Without knowledge of the password for an account or set of accounts, an adversary may systematically guess the password using a repetitive or iterative mechanism. Brute forcing passwords can take place via interaction with a service that will check the validity of those credentials or offline against previously acquired credential data, such as password hashes. Brute forcing credentials may take place at various points during a breach. For example, adversaries may attempt to brute force access to [Valid Accounts](https://attack.mitre.org/techniques/T1078) within a victim environment leveraging knowledge gathered from other post-compromise behaviors such as [OS Credential Dumping](https://attack.mitre.org/techniques/T1003), [Account Discovery](https://attack.mitre.org/techniques/T1087), or [Password Policy Discovery](https://attack.mitre.org/techniques/T1201). Adversaries may also combine brute forcing activity with behaviors such as [External Remote Services](https://attack.mitre.org/techniques/T1133) as part of Initial Access.

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

T1003

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.

Url

Value
http://89.117.2.34/4qp/8Y.txt
http://89.117.2.34/3m3sxh6/IuM.txt
http://89.117.2.33/hvwsuw/udrh.txt
http://89.117.2.33/7ipw/7ohq.txt
http://89.117.1.161/mtdi/ZQCw.txt
http://89.117.1.161/epxq/A.txt
http://89.117.1.160/zkf2r4j/VmD.txt
http://89.117.1.160/4bvt1yw/iC.txt
http://85.239.33.149/naams/p3aV.txt
http://66.63.188.19/bmkmsw/2.txt
http://176.123.2.146/vbcsn/UOx.txt
http://176.123.2.146/5aohv/9mn.txt
http://155.94.208.137/tgnd/zH9.txt

http://146.19.213.36/vei/yEZZ.txt

http://146.19.213.36/dbna/H.txt

http://104.129.20.167/xhsmd/bOWEU.txt

http://103.124.106.224/uuny19/bb1nG.txt

http://103.124.105.233/yusx/dMA.txt

http://103.124.104.76/wsr6oh/Y.txt

http://103.124.105.208/wha5uxh/D.txt

http://103.124.104.22/zjxb/bO.txt

External References

- https://www.proofpoint.com/us/blog/threat-insight/ta577s-unusual-attack-chain-leads-ntlm-data-theft
- https://otx.alienvault.com/pulse/65e5ddaf15b7ce8a1002ca09