Jun 11 2023

NETMANAGEIT

Intelligence Report

Threat Actors Using Fake QuickBooks Software to Scam Organizations

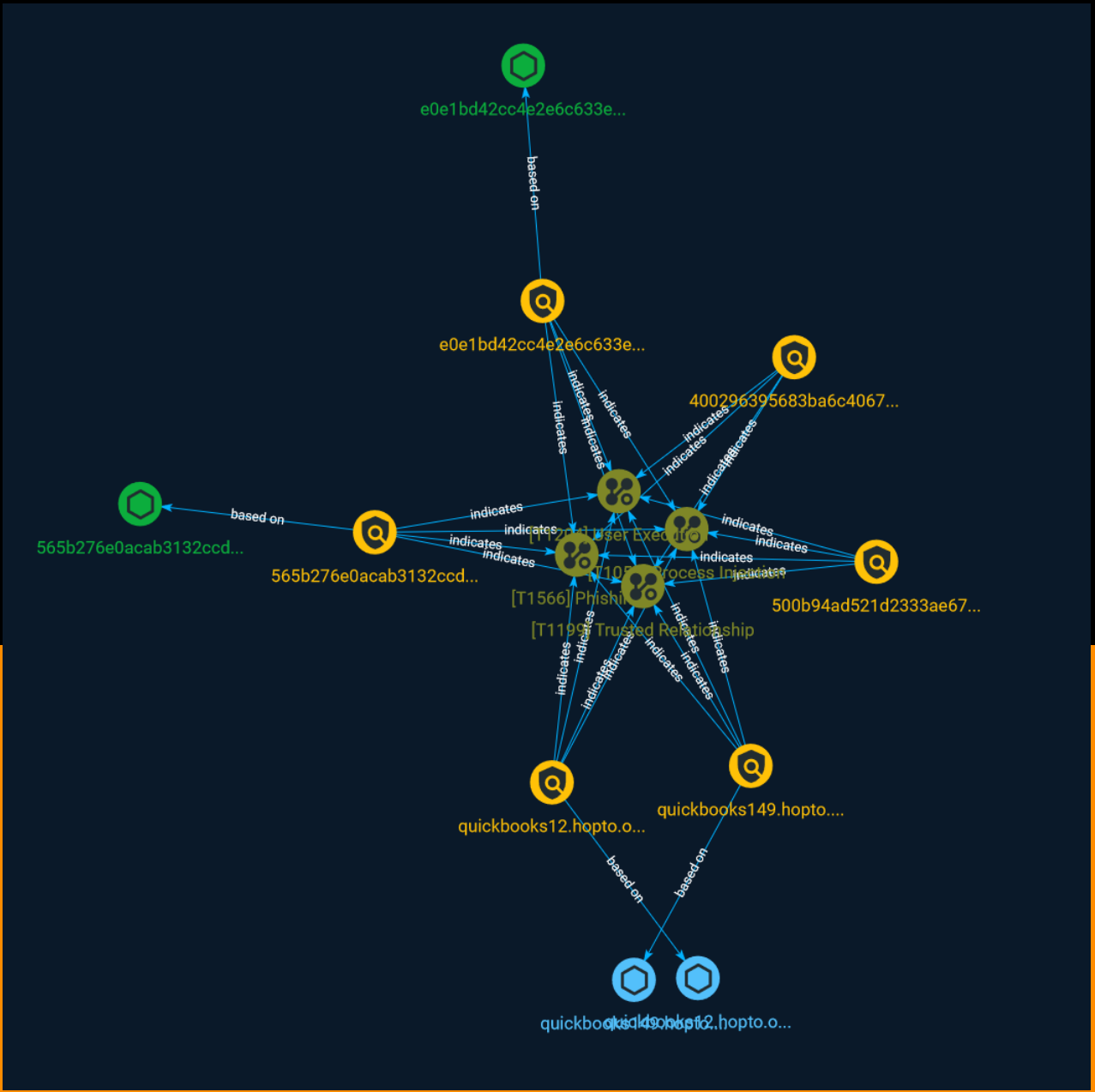

Table of contents

Overview

Entities

Observables

External References

Overview

Description

The QuickBooks scam has been identified as a known threat, with concerned users posting messages on Reddit and QuickBooks forums about warning messages and non-legitimate support services being offered.

Confidence

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

15 / 100

Attack-Pattern

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
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

User Execution

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

Trusted Relationship

ID

T1199

Description

Adversaries may breach or otherwise leverage organizations who have access to intended victims. Access through trusted third party relationship abuses an existing connection that may not be protected or receives less scrutiny than standard mechanisms of gaining access to a network. Organizations often grant elevated access to second or third-party external providers in order to allow them to manage internal systems as well as cloud-based environments. Some examples of these relationships include IT services contractors, managed security providers, infrastructure contractors (e.g. HVAC, elevators, physical security). The third-party provider's access may be intended to be limited to the infrastructure being maintained, but may exist on the same network as the rest of the enterprise. As such, [Valid Accounts](https://attack.mitre.org/techniques/T1078) used by the other party for access to internal network systems may be compromised and used. (Citation: CISA IT Service Providers) In Office 365 environments, organizations may grant Microsoft partners or resellers delegated administrator permissions. By compromising a partner or reseller account, an adversary may be able to leverage existing delegated administrator relationships or send new delegated administrator offers to clients in order to gain administrative control over the victim tenant.(Citation: Office 365 Delegated Administration)

Sector

Name
Finance
Description
Public and private entities involved in the allocation of assets and liabilities over space and time.
Name
Consulting
Description
Private entities providing expert advice in a specific field to external entities.

Indicator

Name
quickbooks12.hopto.org
Pattern Type
stix
Pattern
[hostname:value = 'quickbooks12.hopto.org']
Name
e0e1bd42cc4e2e6c633e919542014bb2adfe64008dc02457eb5da350c905459b
Description
stack_string SHA256 of fedaef3bbafbd89d38f1061052da4f8b
Pattern Type
stix
Pattern

[file:hashes.'SHA-256' = 'e0e1bd42cc4e2e6c633e919542014bb2adfe64008dc02457eb5da350c905459b']

Name

500b94ad521d2333ae6792521ee28f04d2927bb6

Description

QuickBooks scamming malware

Pattern Type

yara

Pattern

rule QuickBooks_RuntimeBokers { meta: author = "eSentire TI" description = "QuickBooks scamming malware" date = "4/27/2023" strings: $s1 = "C:\\Users\\Public\\Libraries\\sv.ini" $s2 = "C:\\Users\\Public\\Libraries\\err.bin" $s3 = "quickbooks12.hopto.org" $s4 = "quickbooks149.hopto.org" $s5 = "C:\\Users\\Public\\Libraries\\QBD.exe" wide condition: all of ($s*) and filesize < 400KB and (uint16(0) == 0x5A4D or uint32(0) == 0x4464c457f) }

Name

565b276e0acab3132ccde2a68fb8e948270261867188fb63953a5331be190ba5

Description

stack_string SHA256 of 39a0b4c7287cecc915ab2449669923dd

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '565b276e0acab3132ccde2a68fb8e948270261867188fb63953a5331be190ba5']

Name

400296395683ba6c4067d128e17701c1938d8249

Description

QuickBooks scamming malware

Pattern Type

yara

Pattern

rule QuickBooks_QBD { meta: author = "eSentire TI" description = "QuickBooks scamming malware" date = "4/27/2023" strings: $s1 = "\\err.html" wide $s2 = "C:\\Users\\Simran\\Desktop\\TEST TESt TES\\QuickBooksDownloder\\obj\\Release\\QBD.pdb" $s3 = "D:\\Side\\QuickBook_23\\Downloader\\QuickBooksDownloder\\obj\\Release\\QBDownloder.pdb" $s4 = "http://185.161.211.237/" wide $s5 = "90s.rtf" wide $s6 = "err.bin" wide condition: 4 of ($s*) and filesize < 700KB }

Name

quickbooks149.hopto.org

Pattern Type

stix

Pattern

```
[hostname:value = 'quickbooks149.hopto.org']
```

StixFile

Value
565b276e0acab3132ccde2a68fb8e948270261867188fb63953a5331be190ba5
e0e1bd42cc4e2e6c633e919542014bb2adfe64008dc02457eb5da350c905459b

Hostname

Value
quickbooks149.hopto.org
quickbooks12.hopto.org

External References

- https://www.esentire.com/blog/threat-actors-using-fake-quickbooks-software-to-scam-organizations
- https://otx.alienvault.com/pulse/64639447e7b0053fdb137ecd