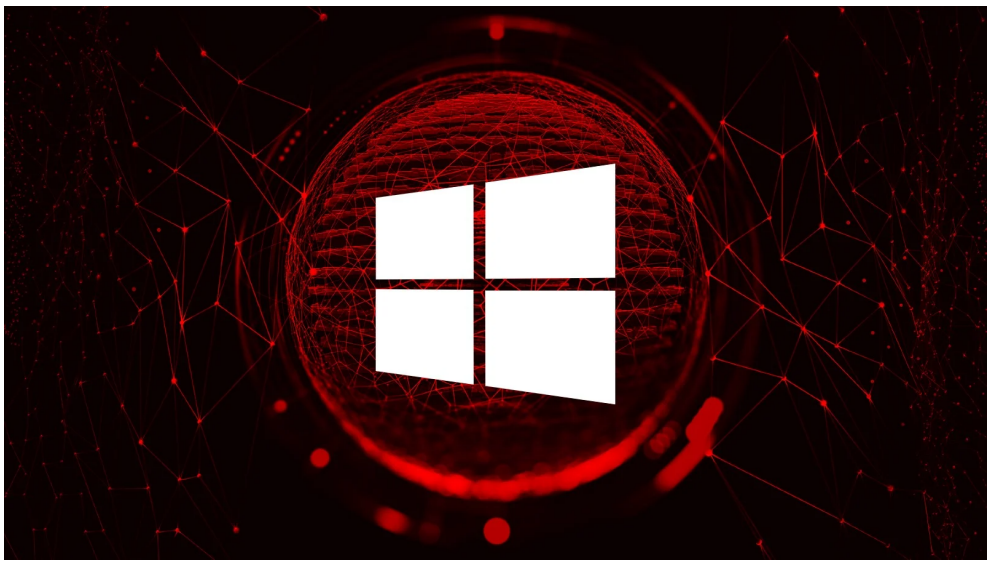
Hacked sites push TeamViewer using fake expired certificate alert

By **Sergiu Gatlan (https://www.bleepingcomputer.com/author/sergiu-gatlan/)** September 20, 2021 04:15 PM **0**



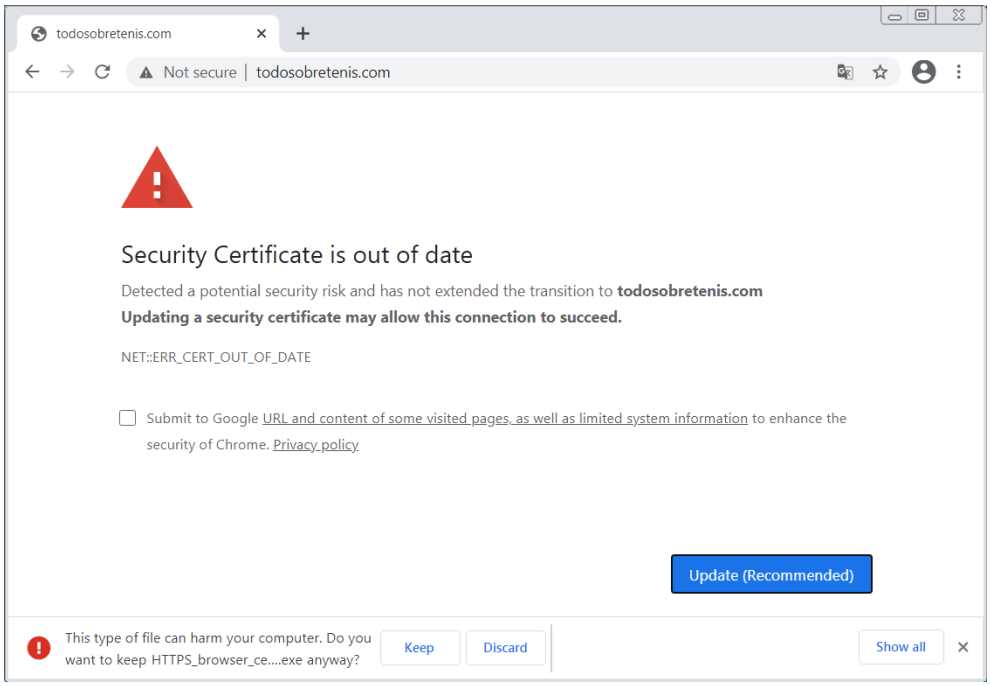
Threat actors are compromising Windows IIS servers to add expired certificate notification pages that prompt visitors to download a malicious fake installer.

Internet Information Services (IIS) is Microsoft Windows web server software included with all Windows versions since Windows 2000, XP, and Server 2003.

The message shown on the malicious certificate expiration error pages reads: "Detected a potential security risk and has not extended the transition to [sitename]. Updating a security certificate may allow this connection to succeed. NET::ERR_CERT_OUT_OF_DATE."

AD

As Malwarebytes Threat Intelligence security researchers observed (https://twitter.com/MBThreatIntel/status/1439995792693944324.), the malware installed via a fake update installer [VirusTotal (http://www.virustotal.com/gui/file/223d8c94877ac7e689733ab7131b749393c7570c2653cd1955f5cb2b4d68deae/detection)] signed with a Digicert certificate.



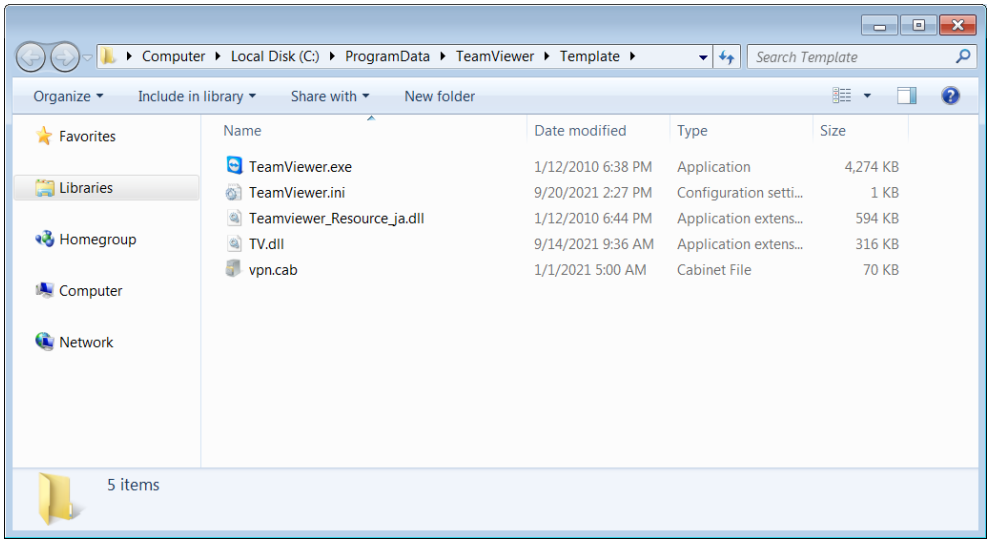
Malicious page hosted on hacked IIS server

The payload dropped on infected systems is TVRAT (https://malpedia.caad.fkie.fraunhofer.de/details/win.teamspy) (aka TVSPY, TeamSpy, TeamViewerENT, or Team Viewer RAT), a malware designed to provides its operators with full remote access to infected hosts.

Once deployed on infected device, the malware will silently install and launch an instance of the TeamViewer remote control software.

After being launched, the TeamViewer server will reach out to a command-and-control (C2) server to let the attackers know they can remotely take complete control of the newly compromised computer.

TVRAT first surfaced in 2013 (https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=75705e7f-749d-4052-ae24-5531d93d8613&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments) when it was delivered via spam campaigns as malicious attachments that tricked targets into enabling Office macros.



TeamViewer installed by TVRAT

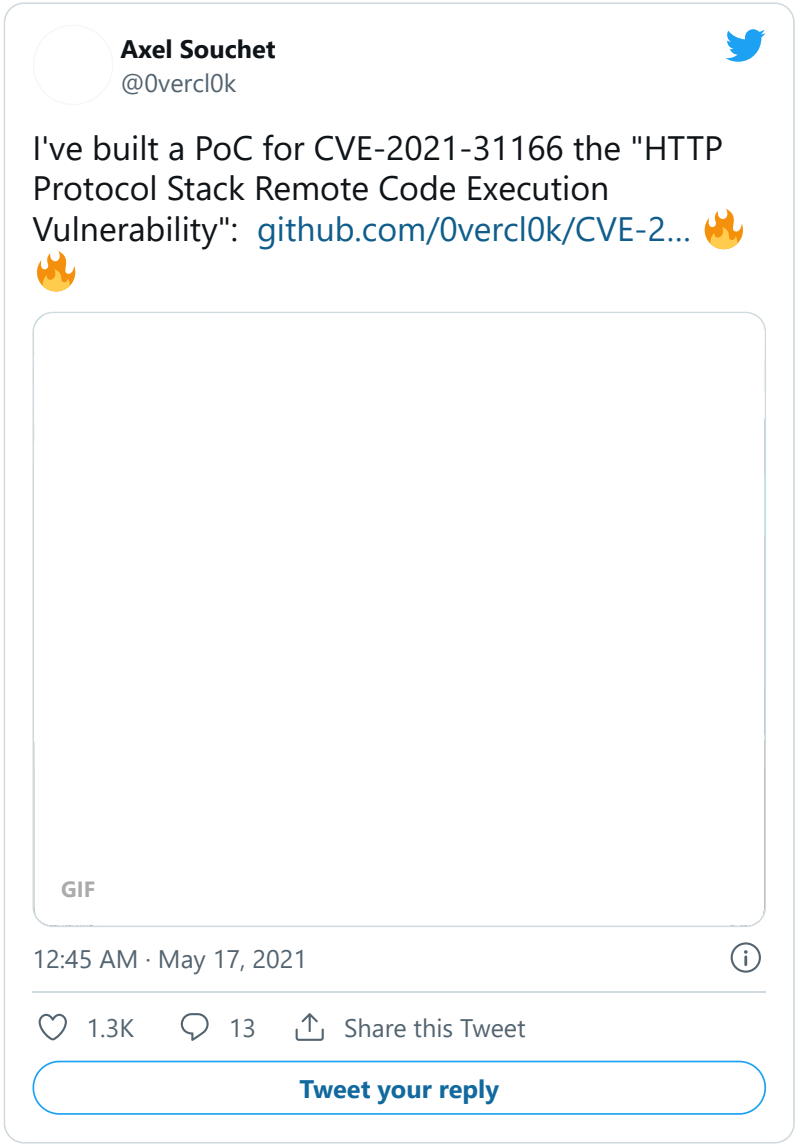
IIS servers: vulnerable and targeted

While the method used by the attackers to compromise IIS servers is not yet known, attackers can use various ways to breach a Windows IIS serverr.

For instance, exploit code targeting a critical wormable vulnerability found in the HTTP Protocol Stack (HTTP.sys) used by the Windows IIS web server has been publicly available since May (https://www.bleepingcomputer.com/news/security/exploit-released-for-wormable-windows-http-vulnerability/).

Microsoft patched the security flaw (tracked as CVE-2021-31166) during the May Patch Tuesday and said it only impacts Windows 10 versions 2004/20H2 and Windows Server versions 2004/20H2.

There hasn't been any malicious activity abusing this flaw in the wild since then and, as we reported at the time, most potential targets were likely safe from attacks given that home users with the latest Windows 10 versions would've updated and companies don't commonly use the latest Window Server versions (https://twitter.com/GossiTheDog/status/1392211087601410054).



However, state-sponsored level threat actors have also leveraged various other exploits to compromise internet-facing IIS servers in the past.

The most recent example is an advanced persistent threat (APT) group tracked as Praying Mantis or TG1021, which targeted Microsoft IIS web servers (https://f.hubspotusercontent30.net/hubfs/8776530/TG1021%20-%20Praying%20Mantis%20Threat%20Actor.pdf) according to an August report from Israeli security firm Sygnia.

In their attacks, Praying Mantis used a Checkbox Survey RCE Exploit (CVE-2021-27852), a VIEWSTATE Deserialization and Altserialization Insecure Deserialization exploits, and a Telerik-UI Exploit (CVE-2019-18935, CVE-2017-11317).

"The operators behind the activity targeted Windows internet-facing servers, using mostly deserialization attacks, to load a completely volatile, custom malware platform tailored for the Windows IIS environment," the researchers said.

Praying Mantis actors then used the access the hacked IIS servers provided to conduct additional malicious tasks, including credential harvesting, reconnaissance, and lateral movement on their targets' networks.

Related Articles:

OMIGOD: Microsoft Azure VMs exploited to drop Mirai, miners (https://www.bleepingcomputer.com/news/security/omigod-microsoft-azure-vms-exploited-to-drop-mirai-miners/)

New malware uses Windows Subsystem for Linux for stealthy attacks (https://www.bleepingcomputer.com/news/security/new-malware-uses-windows-subsystem-for-linux-for-stealthy-attacks/)

New Zloader attacks disable Windows Defender to evade detection (https://www.bleepingcomputer.com/news/security/new-zloader-attacks-disable-windows-defender-to-evade-detection/)

Ukrainian extradited for selling 2,000 stolen logins per week (https://www.bleepingcomputer.com/news/security/ukrainian-extradited-for-selling-2-000-stolen-logins-per-week/)

Synology warns of malware infecting NAS devices with ransomware (https://www.bleepingcomputer.com/news/security/synology-warns-of-malware-infecting-nas-devices-with-ransomware/)