Foundations of Cybersecurity
Final Project and Report

Quasar RAT C&C Data Theft

Prepared by Ethan Couch
UID: U79532295

Table of Contents

Abstract

The following report works to describe a recent Florida-based cyber attack that illicitly captures the credentials of legally-authorized medical marijuana cardholders for unlawful distribution under the discretion of an amateur cybercrime agency. This agency operates under the intentions to use stolen medical marijuana card details to forge fraudulent/counterfeit copies of such cards for auction to a wealth of dark-web buyers. The presumed Floridian cybercrime agency employs phishing and website forgery protocols to manipulate legitimate medical marijuana cardholders into revealing all required information for creating a medical identification card for legal purchase and use of medical cannabis at Miami-based dispensaries, under the impersonation of each patient's medical provider. Lastly, this criminal organization markedly uses tools such as **King Phisher (open source phishing campaign tool),** numerous phishing kits modeled after Florida's insurance websites, and a private command and control server to coordinate and monitor their phishing attack before, during, and after execution of the campaign.

In this document the phases of the attack will be broken down using the DHS "Kill Chain", which is represented below:

Scenario Introduction

As a byproduct of the COVID-19 pandemic, we can assign the thankless statistic of 600% increase in cybercrime to the world's current cyberscape (2019 cyber SECURITY Statistics trends & data). As the COVID-19 pandemic sweeps across many of today's digitally-sophisticated nations, much of the world's professional and social activity has been pushed to online and remote formats, where 98% of concentrated cyber attacks implement social engineering practices to coordinate data breaches and theft. With this dramatic influx of criminal cyber activity, it is now that we can look at the social-engineering-fueled damages caused by a criminal cybersecurity organization named Cartec; an organization acting to exploit the conditions of medical marijuana obtainment within the United States through the establishment of a Silk Road portal that sells counterfeit replicas of real patients' medical marijuana cards and documents, for monetary gain towards the expansion of their company and illegal drug ascertainment services.

Threat Actor

The threat actor within this campaign has been identified as a Floridian cyberintelligence agency, in which works under the presumed name of 'Cartec,' having ties with illegal drug-trafficking services/web portals within the dark web.

Target

The target for this documented attack is the Floridian medical cannabis industry, though the exact exploited target trickles down to that of a previously documented vulnerability within Sydent (CVE-2021-29432).

Campaign

A certain medical market is experiencing tremendous traction in both its access from medical patients wielding legitimate prescriptions, and unfortunately, cybercrime agencies wielding exploitative intentions. The medical cannabis industry, in conjunction with the vulnerable digital atmosphere that the recent pandemic has brought about, has become subject to numerous social-engineering attacks by cyber threat actor 'Cartec.' Cartec begins their campaign by preparing a phishing attack under the tool **King Phisher**, as well as by exploiting a vulnerability within Sydent, a reference matrix identity server. Cartec plans to use Sydent to send out endless phishing emails from an obscure Sydent email address, allowing them to continuously construct inconspicuous phishing emails. King Phisher is important as it allows Cartec a consistently updated planning and results-based interface for their phishing attack; it provides them features ranging from the crafting of an initial phishing email and attachment, to a seamless integration of spoofed websites to be hosted on a remote server, all while providing statistics of each affected victim. Once Cartec has crafted a suitable format for their campaign through the use of King Phisher, they must ensure immediate contact with patients who have recently received designated identification records regarding prescribed use of marijuana. Cartec contacts each applicable patient with a weaponized email that contains various spoofed websites created from phishing kits; ultimately, all of the website addresses linked within the email are hosted by a Cartec-owned command and control server, in which will execute malicious code as a response to the Quasar trojan installment (occurs upon click of spoofed website)that copies information typed into the webpage, in order to store stolen medical marijuana card details after tricking the patient into entering such details as compliance to their health insurance provider.

The Exploit

Prior to the initiation of their campaign, Cartec researches the TTPs of phishing attacks, and come to the conclusion that they will employ a notable remote access trojan (RAT) 'Quasar' that executes on a user system when clicking an email-attached link to a spoofed website hosted by a server that Cartec has command and control access over, and Quasar, communication permissions with.

Stages of the Attack

Reconnaissance

Cartec executes their campaign by first analyzing data gathered from a social engineering process that connects a small network of corrupt medical workers within select independent medical practices in Miami. These medical workers fulfill amateur and unsuspecting roles in each practice, and conveniently demand little pay from Cartec for their illegal cooperation in divulging patients' personal information. Nonetheless, these low-level assistants consistently relay to the threat actors at Cartec the contact details of each patient who has recently obtained a prescription for medical marijuana through their supervisor.

Weaponizing

Following the process outlined to them by their focused exploit, Cartec must ensure that they are able to formulate multiple spoofed websites that mimic the Floridian health insurance websites that a patient may commonly use. To do this, Cartec acquires multiple phishing kits marketed for use in targeting insurance companies such as Florida Blue, Blue Cross Blue Shield, and Ambetter. Utilizing the company's tie with dark web phishing kit developers, Cartec soon has all the HTML, images, and code needed to create fraudulent sites for each notable insurance company. With the help of each custom phishing kit, Cartec hosts each of these spoofed websites and their addresses on the company's private command and control server to await delivery. Of course, this command and control server further interacts with the Quasar RAT that is bundled and installed with the clicked link, in order to assign Quasar an executive role in the data copy and transposition of user information that is entered within the spoofed website link. The Quasar RAT's presence is marked by a 'jli.dll' file, though the inclusion of this executable is hidden from the link clicker.

Delivery

After receiving the contact information (emails) of each medical marijuana candidate, Cartec sends each applicable patient a weaponized email that urgently mandates the need for each patient to verify their medical marijuana documentation with their health insurance provider. Each email is deliberately crafted to appear as if it originates from the practitioner the patient recently visited. For this reason, the CVE-2021-29432 vulnerability and Sydent as a whole play a much greater role in the overall execution of Cartec's phishing malware attack's delivery than might be expected. To verify this required information, The phishing emails inform the individual to click a contained link (resembling the domain address of the actual insurance website)that redirects to a cloned website of the individuals relevant insurance provider; after clicking the link pertaining the supposed website of their health insurance provider, the patient is then prompted to verify all details of their recently assigned medical marijuana card as part of the terms of their insurance policy.

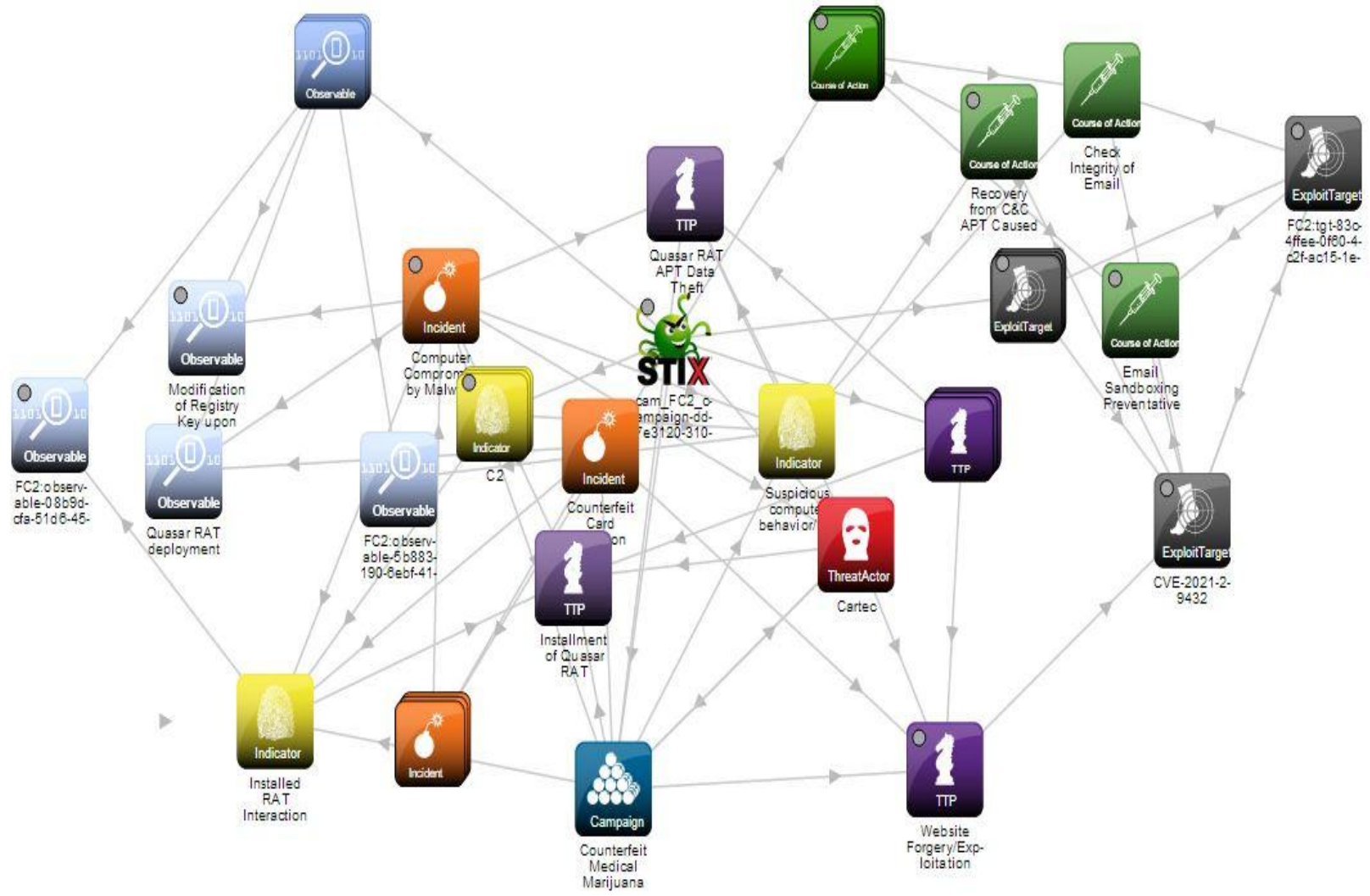
Exploit

The user's machine is specifically exploited first by the download of the jli.dll executable, which invokes the Quasar RAT that communicates copied spoofed web page information to Cartec's command and control server. Of course, this is not possible without the initial exploit employed with Cartec, which

incites use of a Sydent vulnerability (CVE-2021-29432) to craft an email with domain references that are untraceable and otherwise unsuspecting.

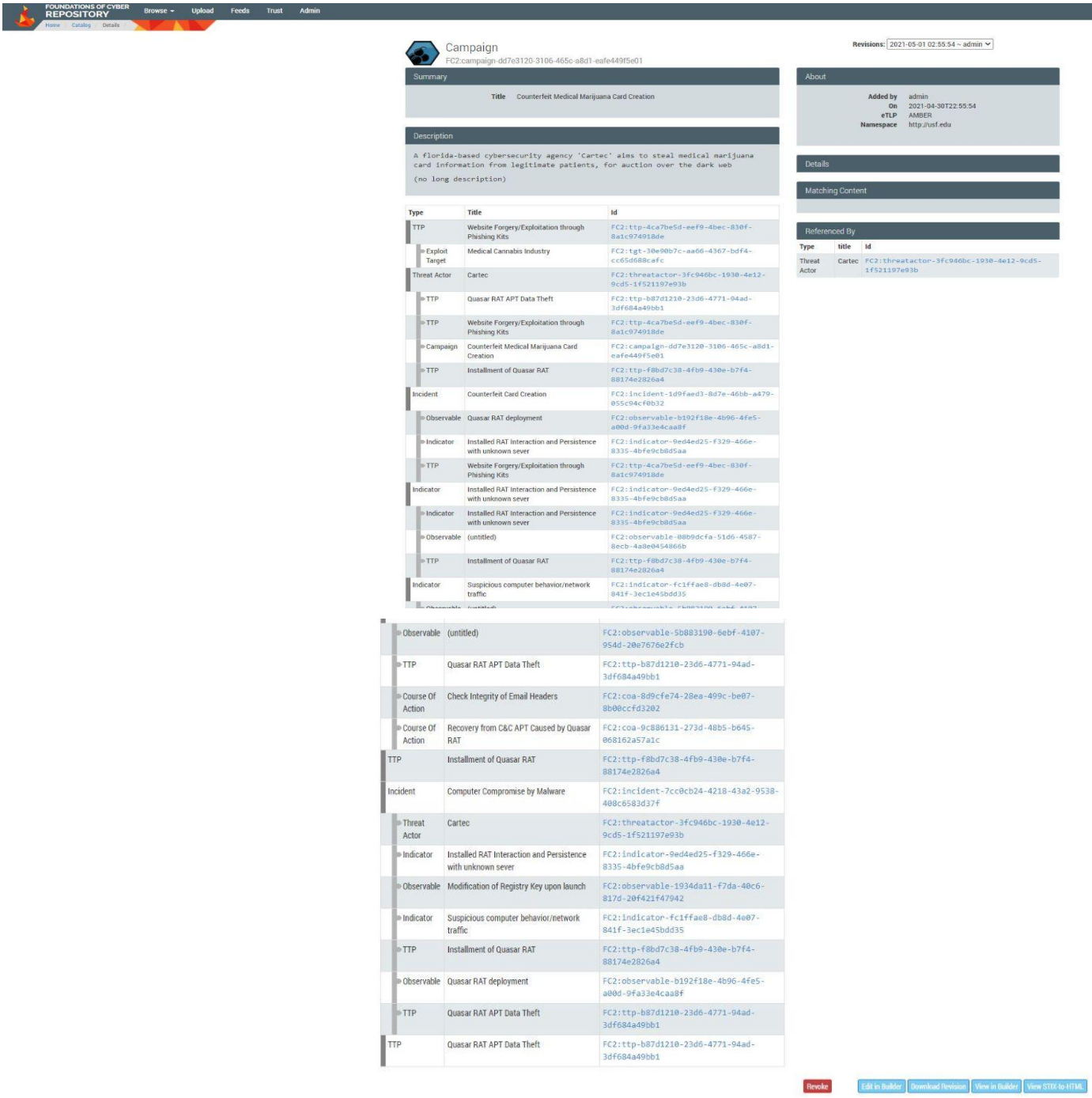
Stix Viz Representation

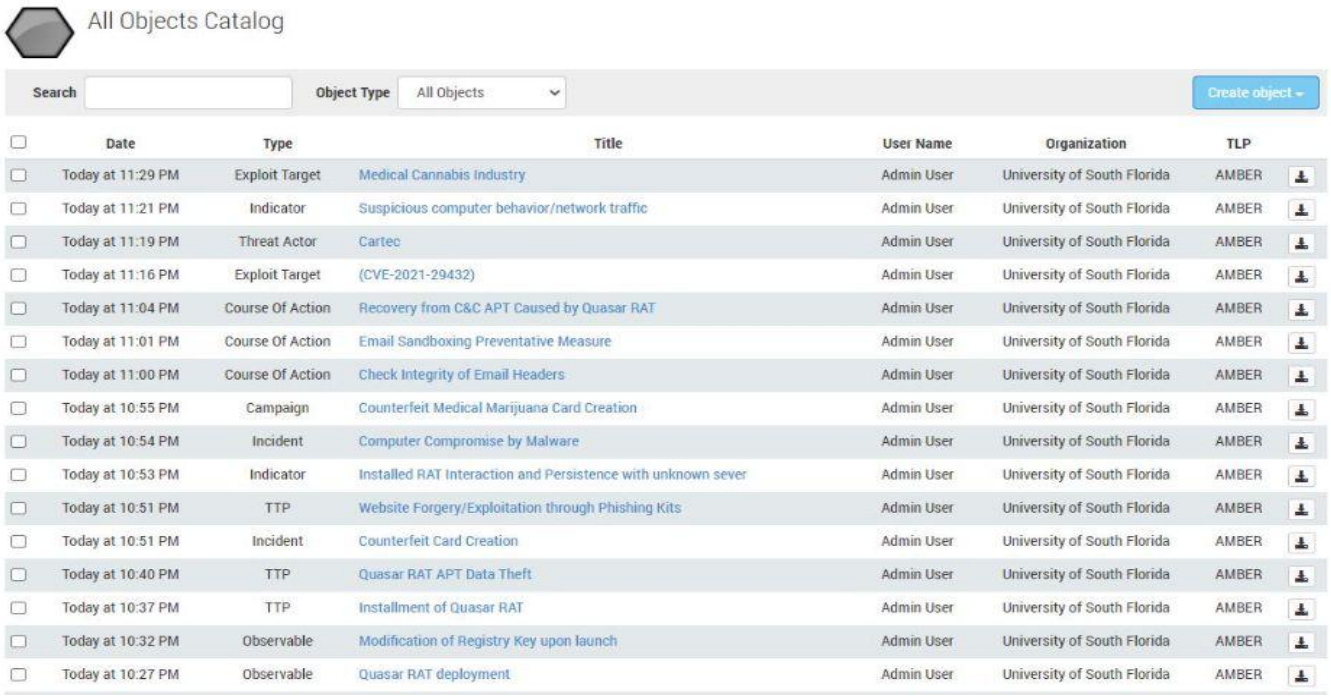
Quasar RAT C&C Data Theft Phishing Attack in StixViz image below:



Soltra/Edge Representation

Quasar RAT C&C Data Theft Phishing Attack in Soltra/Edge image below:





All Objects Catalog

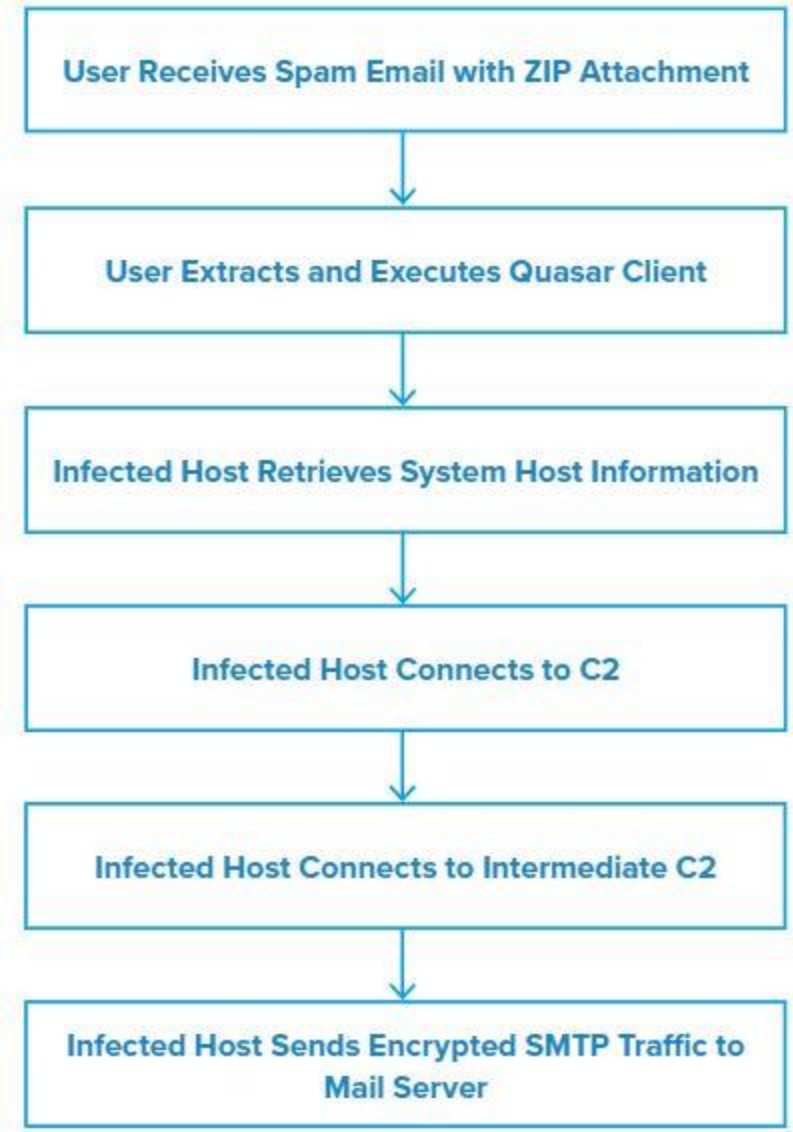
Search | Object Type: All Objects | Create object

Date	Type	Title	User Name	Organization	TLP
Today at 11:29 PM	Exploit Target	Medical Cannabis Industry	Admin User	University of South Florida	AMBER
Today at 11:21 PM	Indicator	Suspicious computer behavior/network traffic	Admin User	University of South Florida	AMBER
Today at 11:19 PM	Threat Actor	Cartec	Admin User	University of South Florida	AMBER
Today at 11:16 PM	Exploit Target	(CVE-2021-29432)	Admin User	University of South Florida	AMBER
Today at 11:04 PM	Course Of Action	Recovery from C&C APT Caused by Quasar RAT	Admin User	University of South Florida	AMBER
Today at 11:01 PM	Course Of Action	Email Sandboxing Preventative Measure	Admin User	University of South Florida	AMBER
Today at 11:00 PM	Course Of Action	Check Integrity of Email Headers	Admin User	University of South Florida	AMBER
Today at 10:55 PM	Campaign	Counterfeit Medical Marijuana Card Creation	Admin User	University of South Florida	AMBER
Today at 10:54 PM	Incident	Computer Compromise by Malware	Admin User	University of South Florida	AMBER
Today at 10:53 PM	Indicator	Installed RAT Interaction and Persistence with unknown sever	Admin User	University of South Florida	AMBER
Today at 10:51 PM	TTP	Website Forgery/Exploitation through Phishing Kits	Admin User	University of South Florida	AMBER
Today at 10:51 PM	Incident	Counterfeit Card Creation	Admin User	University of South Florida	AMBER
Today at 10:40 PM	TTP	Quasar RAT APT Data Theft	Admin User	University of South Florida	AMBER
Today at 10:37 PM	TTP	Installment of Quasar RAT	Admin User	University of South Florida	AMBER
Today at 10:32 PM	Observable	Modification of Registry Key upon launch	Admin User	University of South Florida	AMBER
Today at 10:27 PM	Observable	Quasar RAT deployment	Admin User	University of South Florida	AMBER

Install

In order for the effective use of their private command and control server, Cartec recognizes that they must ensure reliable and deliberate installation of the Quasar malware object onto each individual's system, at the click of a link. Cartec decides that the link, as stated before, will contain a bundled executable 'jli.dll' in which will discretely install the remote access trojan upon the exploited patient's visitation of what they perceive to be a genuine website hosted on a genuine domain.

To better flesh out the details of this process, Cartec evaluates and employs following intricacies of the Quasar RAT that they divulged from a threat report intelligence resource (source: https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--42):



Following this outline, Cartec takes the following steps to configure the Quasar RAT for their campaign:

1. Drop the Quasar clients in the victim's 'C:\Users\admin\AppData\Roaming\' directory, written as 'jli.dll', upon the click of a bundled link attachment.
2. The server client builder limits the folder locations in which clients are placed to the base directories %APPDATA%, Program Files, and Windows\SysWOW64.
3. The network behavior and traffic data mirrors the Quasar v1.3.0.0 discrete installation.
4. The executable modifies the value of the exploited patient's Windows registry key at HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

to automatically run Quasar clients during Windows launch. This is a precaution that Cartec applies to ensure some level of persistence of their trojan.

5. The Quasar trojan executes additional processes that connect Cartec's C&C server with encrypted SMTP traffic from the infected host to a mail server that is exploited from the previously defined Sydent vulnerability, allowing otherwise plausible appearance of emails from the victim's perspective.

Command and Control

As an integral part of the campaign's success, Cartec must use the command and control server that hosts each of their spoofed websites as a data retrieval mechanism. Given that each recipient of the phishing email clicks on one of the links to a malicious spoofed website and download of Quasar RAT, communication with Cartec's universal command and control server is instantiated, as well as the execution of malicious code for the upload of the sensitive credentials captured for Quasar RAT. From this point, the command and control server copies all user-entered card details on the spoofed website as a response to the RAT infection that spawns from the initial click of a link by the email recipient.

Actions on Objectives

Unbeknownst to the victim, each cloned health insurance website had been made to mirror all elements of various Florida health insurance sites, with the exception being that each spoofed site was being hosted on a private server rented by Cartec for storing and eventual retrieval of the user's entered details. Through this process, Cartec is able to build a consistently growing catalogue of valid medical marijuana card credentials, in which they will use to create and sell counterfeit copies of these cards over the dark web, specifically through Silk Road listings.

Incident Handling Process

Identification Phase

Given the amount of research and reconnaissance that are incorporated into spear phishing attacks (like Cartec's), identification of the occurrence or possibility of such an attack can be considerably difficult. Regardless, identification of Cartec's phishing attack is possible through careful analysis of the weaponized email used in Cartec's campaign.

Specifically, recipients of such an email can hover over any included links to infer the legitimacy of the linked domain address using tools that check the integrity of a domain name. Additionally, the recipient of the email should analyze email headers to check if all parameters of the email lead to the same domain stated in the email.

Lastly, it may be possible to identify an attempted phishing attack by unusual changes to the computer's performance and behavior, in which, in this case, may be indicative of the webpage's discrete communication with a command and control server.

On another front, Cartec's use of the Quasar RAT provides much more obvious indicators of a system compromise, in which can be traced through network traffic capturing programs such as FireEye. Efforts to dismantle a RAT phishing attack are documented in the following reference, in which proved successful with careful attention to network traffic upon clicking a malicious link bundled with a RAT executable. Further, these Quasar RAT indicators are commonly existent with file loader variants such as Jjs.exe, jli.dll, Msvcrt100.dll, and svchost.bin.

(reference:
https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/faas/cs-quasarrat.pdf)

Eradication and Recovery Phase

To protect against the future occurrence of an attack like this, as well as mitigate ongoing damage by Cartec, the medical cannabis industry published a report noting the importance of understanding the protocols of command and control(C&C) server and the context in which they can be used within phishing attacks

(source:

https://www.sans.org/blog/the-importance-of-command-and-control-analysis-for-incident-response/)

Even with repeated success of Cartec's campaign, eradication and recovery may never become viable options if an attack is not first identified to have occurred. Given that Cartec's spear phishing attack included an installment of malware in the form of a remote access trojan (RAT) Quasar, this attack should first look to be mitigated with preventative countermeasures.

Indeed, in this attack, the individual needed to be aware of the threat contained within the suspicious email sent to them with a level of great urgency. By refusing to click on any contained links in the email, or abstaining from entering any confidential credentials into one of the spoofed websites, the command and control server which ultimately enables this attacks success would never be able to catalogue the required information for an ongoing dark web operation that sells data for an agency's monetary gain.

Additionally, the blog post noted above highlights the importance of checking for certain signatures indicative of HTTP/web traffic requests to an unknown command and control server, all of which could be done on a spoofed website page.

Regardless of what Cartec chooses to do with the catalogued medical credentials, precautions should be taken to ensure future attacks cannot occur on the same victim by the same company. Countermeasures of this nature would include installment of software that allows the testing of email content within a virtual environment, preemptive establishment of firewalls which interfere with command and control server operation or malicious code execution, or the victim's renewal/modification of all personal credentials that were subject to compromise in the recognized occurrence of a phishing attack.

Assuming the victim is aware of the use of a RAT in this case, the following courses of action apply, in order to prevent or eradicate the RAT and its C&C connection once on an infected system:

- use unique traffic patterns and proxy log information to detect Quasar activities in their network
- Identify browser user-agent strings that Quasar uses in the proxy server logs. such as "Mozilla/5.0 (Windows NT 6.3; rv:48.0) Gecko/20100101 Firefox/48.0" for querying GeoIP services.
- Determine whether systems are making calls to IP check services during Windows startup.
- Apply some of the Snort signatures related to user-agent strings and traffic payload sizes provided by CISA.8
- Implement reputable antivirus solutions that can detect various RAT executables.

  source: Quasar remote access trojan (rat) - 20191002. (n.d.). Retrieved April 30, 2021, from https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--42

Lessons Learned Phase

Ultimately, the spear phishing attack that Cartec used to incite data theft within a command and control server in communication with a remote access trojan Quasar, brings to light the necessity for users to employ proper critical thinking and analysis to the emails they receive. Ignorance is often the greatest enabler of criminal cyber activity such as is documented in this phishing operation, and so individuals must monitor their communications over digital mediums as if they are responsible for the perpetuation of exploitative cyber attacks with every click of an attachment within an email.

Exploit References

- Sydent
- Quasar RAT
- Phishing Kits (used in website forgery)
- CVE-2021-29432

References

- 2019 cyber SECURITY Statistics trends & data. (2021, March 24). Retrieved April 29, 2021, from https://purplesec.us/resources/cyber-security-statistics/

- Alison Kim. (2021, April 22). Retrieved April 30, 2021, from https://www.sans.org/blog/the-importance-of-command-and-control-analysis-for-incident-response/

- https://nvd.nist.gov/vuln/detail/CVE-2021-29432

- LaVia, P. (2020, August 26). The cannabis industry is under attack by cybercriminals. Retrieved April 30, 2021, from https://pacelavia.medium.com/the-cannabis-industry-is-under-attack-by-cybercriminals-29d78ff782e4

- STIX 2.1 EXAMPLES. (n.d.). Retrieved April 30, 2021, from https://oasis-open.github.io/cti-documentation/stix/examples.html

- https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/faas/cs-quasarrat.pdf

- Quasar remote access trojan (rat) - 20191002. (n.d.). Retrieved April 30, 2021, from https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--42