

TA551: Email Attack Campaign Switches from Valak to IcedID

By Brad Duncan

Published: 2021-01-07 · Archived: 2026-04-05 13:33:18 UTC

Executive Summary

TA551 (also known as Shathak) is an email-based malware distribution campaign that often targets English-speaking victims. The campaign discussed in this blog has targeted German, Italian and Japanese speakers. TA551 has historically pushed different families of information-stealing malware like [Ursnif](#) and Valak. After mid-July 2020, this campaign has exclusively pushed IcedID malware, another information stealer.

This blog provides an overview of TA551, as well as previous activity from this campaign. We also examine changes from this campaign since our previous blog about [TA551 pushing Valak](#) in July 2020.

Palo Alto Networks [Next-Generation Firewall](#) customers are protected from this threat with the [Threat Prevention](#) security subscription, which detects the malware. [AutoFocus](#) customers can track this activity using the [TA551](#) and [IcedID](#) tags.

TA551 Switches to IcedID

We have a [GitHub repository where we track recent TA551 activity](#). The repository contains information on each wave of attack from TA551 since July 6, 2020. Starting on July 14, 2020, we have only seen IcedID malware from these waves of attack.

Since July 14, 2020, these waves of malspam consistently targeted English-speaking victims until [Oct. 27, 2020](#), when we started seeing Japanese templates for the Word documents. TA551 consistently targeted Japanese-speaking victims from Oct. 27-[Nov. 20, 2020](#). After approximately three weeks of Japanese-focused attacks, TA551 switched back to English-speaking victims starting on [Nov. 24, 2020](#).

Regardless of the targeted group, TA551 continues to push IcedID as its malware payload.

History of TA551

We have traced TA551 as far back as February 2019, and since that time, we have noted the following characteristics:

- TA551 has distributed different families of malware, including [Ursnif \(Gozi/ISFB\)](#), [Valak](#) and [IcedID](#).
- TA551 malspam spoofs legitimate email chains based on data retrieved from previously infected Windows hosts. It sends copies of these email chains to recipients of the original email chain.
- The spoofed email includes a short message as the most recent item in the chain. This is a generic statement asking the recipient to open an attached ZIP archive using the supplied password.
- File names for the ZIP archives use the name of the company being spoofed in the email. For example, if the spoofed sender is someone@companyname.com, the ZIP attachment would be named companyname.zip.
- In 2020, we also started seeing emails with info.zip or request.zip as the attached ZIP archive names.
- These password-protected ZIP attachments contain a Word document with macros to install malware.
- File names for the extracted Word documents follow noticeable patterns that have evolved as this campaign has progressed.
- URLs generated by the associated Word macros also follow noticeable patterns that have also evolved as this campaign has progressed.

TA551 in 2019

Figure 8 shows the earliest email we can confirm from this campaign, dated Feb. 4, 2019. It targeted an English-speaking recipient and pushed Ursnif malware.

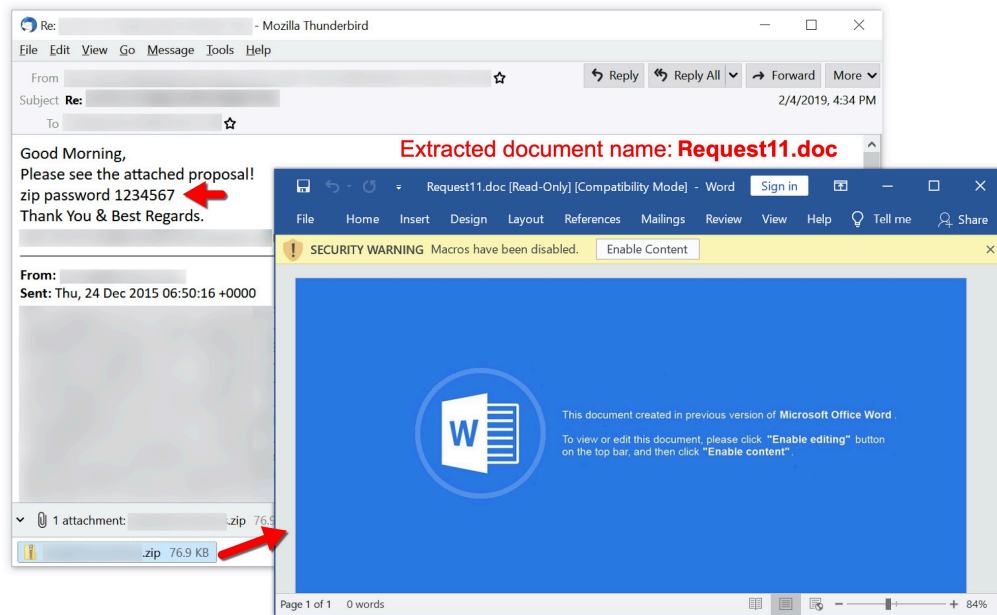


Figure 8. Example of TA551 malspam from February 2019.

The following files are associated with the above example:

- SHA256 hash: 3dab8a906b30e1371b9aab1895cd5aef75294b747b7291d5c308bb19fbc5db10
- File size: 157,696 bytes
- File name: Request11.doc
- File description: Word doc with macro for Ursnif (Gozi/ISFB)
- SHA256 hash: 3afc28d4613e359b2f996b91eeb0bbe1a57c7f42d2d4b18e4bb6aa963f58e3ff
- File size: 284,160 bytes
- File location: hxxp://gou20clair[.]band/xap_102b-AZ1/704e.php?l=zyteb12.gas

File description: Example of Windows EXE retrieved by Word macro – an installer for Ursnif

Figure 9 shows an email from this campaign dated April 2, 2019. It targeted an Italian-speaking recipient and pushed Ursnif malware.

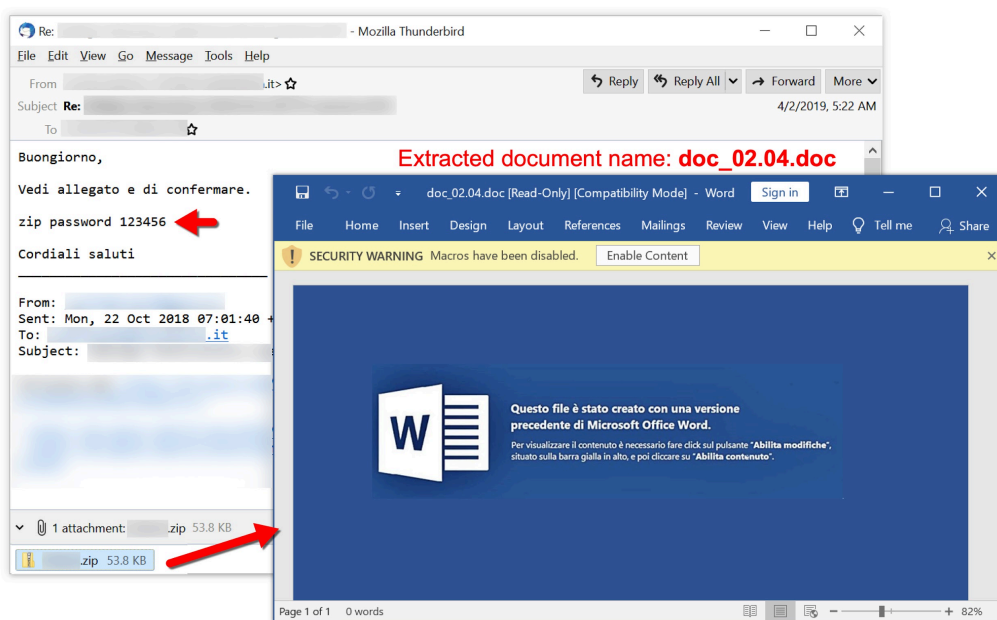


Figure 9. Example of TA551 malspam from April 2019.

The following files are associated with the above example:

- SHA256 hash: 582213137bebc93192b0429f6687c859f007ef03e6a4c620eada8d98ca5d76ba
- File size: 91,136 bytes
- File name: doc_02.04.doc
- File description: Word doc with macro for Ursnif
- SHA256 hash: 8c72d5e5cb81f7a7c2b4881aff3be62cdc09caa52f93f9403166af74891c256e
- File size: 606,208 bytes
- File location: [hxxp://seauj35ywsq\[.\]com/2poef1/j.php?l=zepax4.fgs](https://seauj35ywsq[.]com/2poef1/j.php?l=zepax4.fgs)
- File description: Example of Windows EXE to install Ursnif retrieved by a macro associated with this wave of Word documents

Figure 10 shows an email from this campaign dated Oct. 30, 2019. It targeted a German-speaking recipient and pushed Ursnif malware.

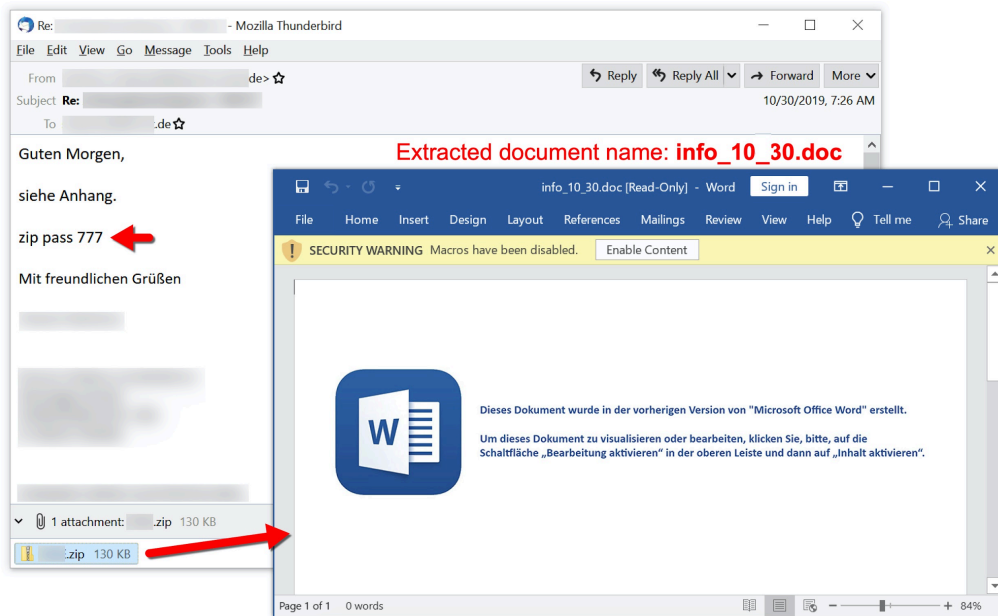


Figure 10. Example of TA551 malspam from October 2019.

The following files are associated with the above example:

- SHA256 hash: 10ed909ab789f2a83e4c6590da64a6bdeb245ec9189d038a8887df0dae46df2a
- File size: 269,312 bytes
- File name: info_10_30.doc
- File description: Word doc with macro for Ursnif
- SHA256 hash: 9e5008090eaf25c0fe58e220e7a1276e5501279da4bb782f92c90f465f4838cc
- File size: 300,032 bytes
- File location: [hxxp://onialisati\[.\]com/deamie/ovidel.php?l=brelry2.cab](https://onialisati[.]com/deamie/ovidel.php?l=brelry2.cab)
- File description: Example of Windows EXE retrieved by Word macro – an installer for Ursnif

Note how the URL from the above example ends in .cab. This pattern was fairly consistent for URLs generated by macros from TA551 Word docs until late October 2020.

Figure 11 shows an email from this campaign dated Dec. 17, 2019. It targeted a Japanese-speaking recipient and pushed Ursnif malware.

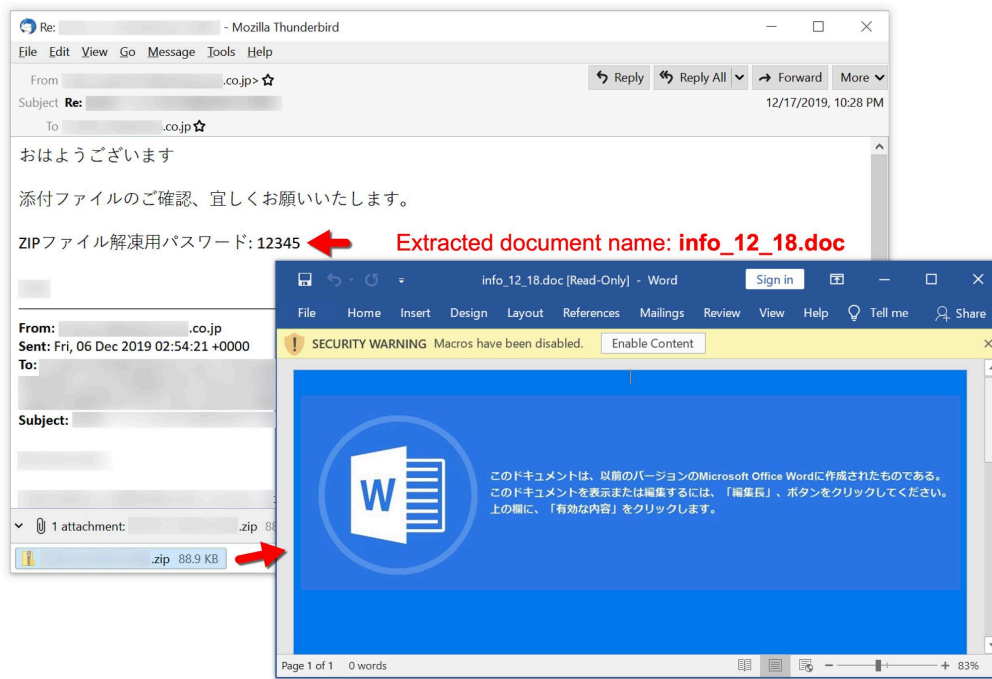


Figure 11. Example of TA551 malspam from December 2019.

The following files are associated with the above example:

- SHA256 hash: 3b28f3b1b589c9a9294099900aa4a01048f2370d03c4da0045aabf61f9e4bb6
- File size: 101,528 bytes
- File name: info_12_18.doc
- File description: Word doc with macro for Ursnif
- SHA256 hash: 3a22d206858773b45b56fc53bed5ee4bb8982bb1147aad9c2a7c57ef6c099512
- File size: 1,650,176 bytes
- File location: hxxp://vestcheasy[.]com/koorsh/soogar.php?l=weecum5.cab
- File description: Example of Windows EXE retrieved by Word macro – an installer for Ursnif

Note that Ursnif-infected hosts [occasionally retrieve follow-up malware](#). For example, on Dec. 19, 2019, a Windows host infected with Ursnif by way of TA551 was also [infected with IcedID and Valak](#) as follow-up malware.

TA551 in 2020

Figure 12 shows an email from TA551 dated March 26, 2020. It targeted a German-speaking recipient and [pushed ZLoader \(Silent Night\) malware](#).

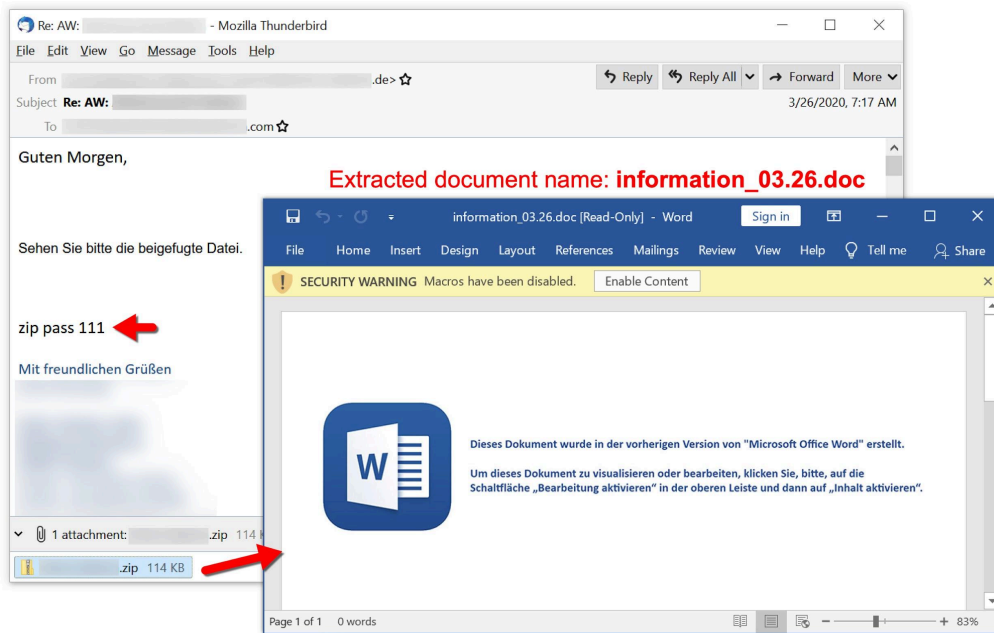


Figure 12. Example of TA551 malspam from March 2020.

The following files are associated with the above example:

- SHA256 hash: 62ecc8950e8be104e250304fdc32748fcadaeaa677f7c066be1baa17f940eda8
- File size: 127,757 bytes
- File name: information_03.26.doc
- File description: Word doc with macro for ZLoader (Silent Night)
- SHA256 hash: 9b281a8220a6098fefe1abd6de4fc126fddfa4f08ed1b90d15c9e0514d77e166
- File size: 486,400 bytes
- File location: hxxp://x0fopmxsq5y2oqud[.]com/kundru/targen.php?l=swep7.cab
- File description: Windows DLL for ZLoader retrieved by Word macro

Figure 13 shows an email from this campaign dated April 28, 2020. It targeted an English-speaking recipient and pushed Valak malware.

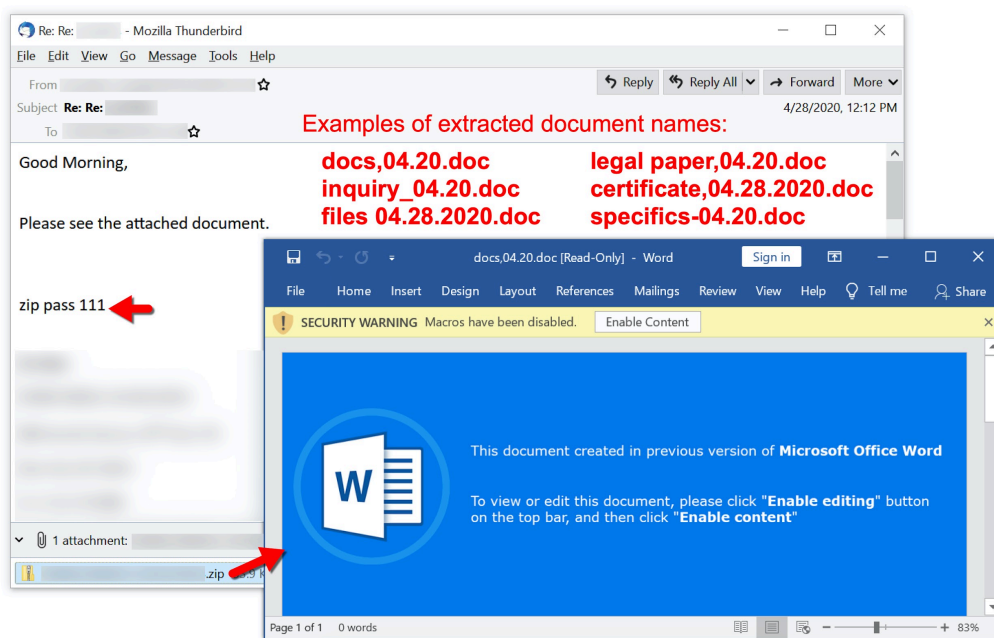


Figure 13. Example of TA551 malspam from April 2020.

The following files are associated with the above example:

- SHA256 hash: bd58160966981dd4b04af8530e3320edbddfc2b83a82b47a76f347d0fb4ca93a
- File size: 61,233 bytes
- File name: docs,04.20.doc
- File description: Word doc with macro for Valak
- SHA256 hash: 9ce4835ef1842b7407b3c8777a6495ceb1b69dac0c13f7059c2fec1b2c209cb1
- File size: 418,816 bytes
- File location: hxxp://qut6oga5219bf00e[.]com/we20lo85/aio0i32p.php?l=nok4.cab
- File description: Example of Windows DLL retrieved by Word macro -- an installer for Valak

At this point, the document names had changed format. This is when we started seeing several different names for the extracted Word documents from each day of attack.

Figure 14 shows an email from this campaign dated May 22, 2020. It targeted an English-speaking recipient and pushed Valak malware.

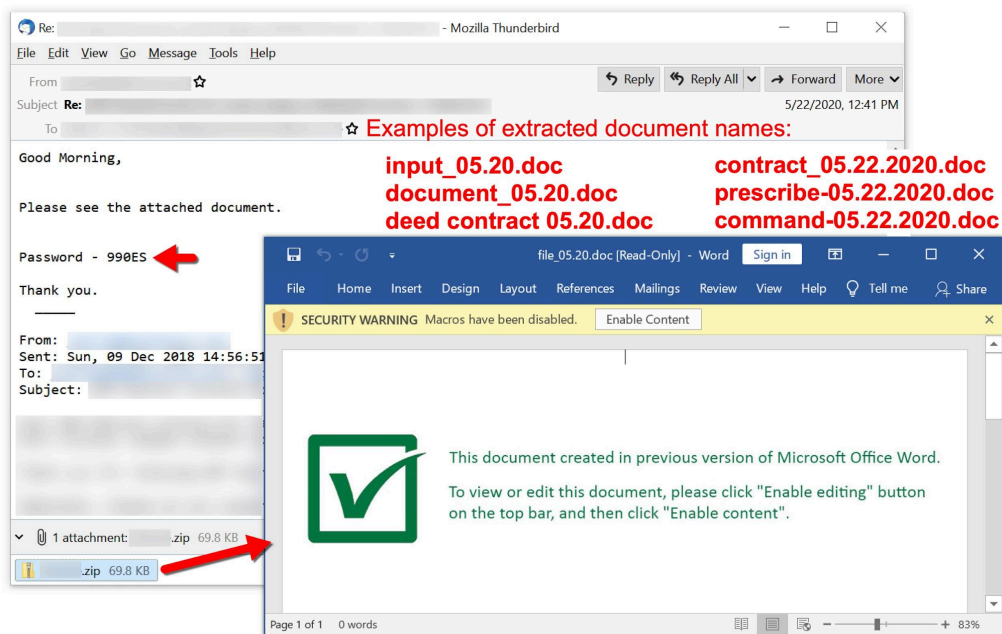


Figure 14. Example of TA551 malspam from May 2020.

The following files are associated with the above example:

- SHA256 hash: 3562023ab563fc12d17981a1328f22a3d3e4c358535b9a0c28173a6e4ad869ba
- File size: 74,338 bytes
- File name: file_05.20.doc
- File description: Word doc with macro for Valak
- SHA256 hash: 4468edc18de42e61b64441c75aedcb15d553410d473e77fc8ae31b358acd506a
- File size: 184,832 bytes
- File location: hxxp://s6oo5atdgmtceep8on[.]com/urvave/cennc.php?l=haao1.cab
- File description: Example of Windows DLL retrieved by Word macro -- an installer for Valak

By this time, the password format for ZIP attachments changed to three digits followed by two letters, and the template style had also been updated.

We continued to see Valak pushed by TA551 through [early July 2020](#). Of note, Valak is a malware downloader, and we frequently saw IcedID as follow-up malware from these infections.

However, by mid-July 2020, TA551 started pushing IcedID directly from the Word document macros.

Recent Developments

In recent weeks, TA551 has changed traffic patterns. For several months prior to [Oct. 19, 2020](#), URLs generated by Word macros to retrieve installer binaries followed a noticeable pattern. This pattern includes:

- .php?l= in the URL path
- URLs end with .cab

Since [Oct. 20, 2020](#), these patterns have changed dramatically. Table 1 shows the changes starting in October.

Date	URL example
2020-10-14	GET /docat/hyra.php?l=dybe18.cab
2020-10-16	GET /muty/sohaq.php?l=tali18.cab
2020-10-19	GET /biwe_zibofyra/ripy_lani.php?l=qedux18.cab
2020-10-20	GET /_bxlzcpijlpkzblf_zhlsplspz/wtlmwrqnnxfwgzzlkvzdbvnp_mphdqpqgxfjvffj_.php?l=chfon4.ppt&lhe=hcqjvtfezhsogtrdxdfs
2020-10-27	GET /update/qqOQccpolFmwCmTnTmURcfZPByI_lqzPNvPftfvLQjqdJtpOYeWT/WRFlVYjJTKqWaf_KhCjsSselY/tbqxj
2020-10-28	GET /update/djMqKxc_BZCF_BJlRmjKmdcihghiSj/wJuzcnBhc/MD/qE_ZWFKbwfWZMCCWgfHU_DNxAcBRIHncRHr/
2020-10-29	GET /update/XTZrbyvClXzcfZcJGZSmDWBthSBXjRKw/cti6
2020-11-03	GET /update/VvZWYoIotoWV_KUywQtEUvUPjvNYMYnLnvWWOLA/fZcXYRwGyzMRZcvzHZrDe/gzlov4
2020-11-04	GET /update/JvYqBVMJCxSDX/nNBk/XhEjPMvaV_dDFIXqGZNCDTLhTXIPWxEsGjTdzfQBUZCvkBqWOgjo/xrei12
2020-11-05	GET /update/jcja/yCGHnwRmyMVTcQljgn/JTHBIVeSrNVdrgJMGGNdiqGxCNACjXDBjkMJKFPKvJNYXFVbcxYvbS/iu
2020-11-19	GET /share/ZSzE0sjR23GkF3VwZi_nqFH2B5lqPUVKxwNC/ahtap3
2020-11-24	GET /share/kvNqzh1tF4Y8zyxL/HQpK6K42Wr8SP9PLJSqxc5h/ROwPcKsG/dbULREqlb1Kj0_RRT/Dfnj/lxnt10

Table 1. URL patterns generated by macros from Word docs distributed by TA551.

By Oct. 27, 2020, URLs generated by TA551 macros include English terms like update or share at the beginning of the HTTP GET request. These URLs end with a series of four to six lowercase English letters followed by a number as low as 1 to as high as 18. These URLs are not consistent in length, and they can be very short or very long.

Since November 2020, we have also noticed [minor changes in artifacts generated during IcedID infections](#), including those outside of the TA551 campaign.

For example, through early November 2020, IcedID DLLs created by installer DLLs were initially saved to the victim's AppData\Local\Temp directory, and the file name started with a tilde (~) and ended with .dll as illustrated earlier in Figure 6.

In November 2020, we started to see a change: the initial IcedID DLLs saved to the victim’s AppData\Local directory with a file name ending in .dat as shown in Figure 15.

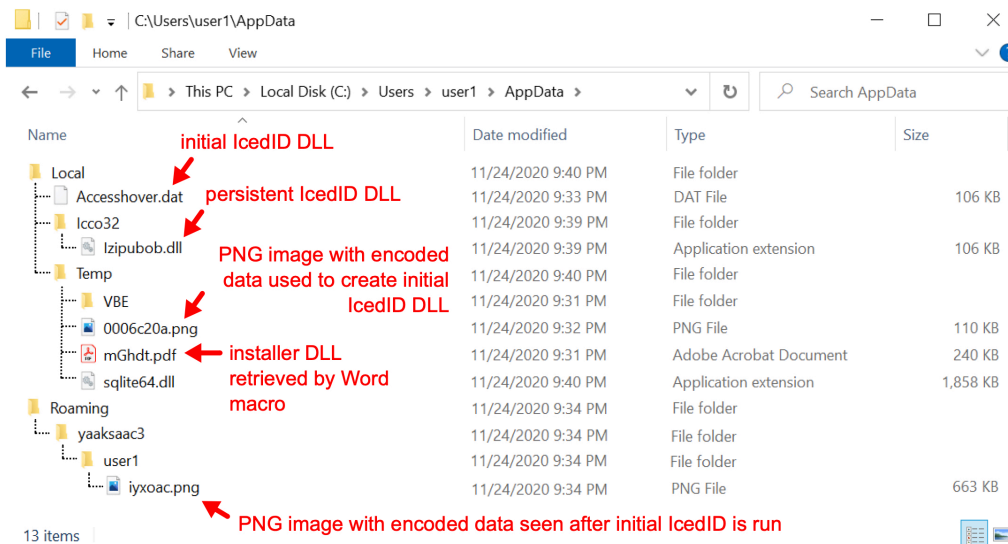


Figure 15. Artifacts seen from a TA551 IcedID infection on Nov. 24, 2020.

These changes may be an effort by malware developers to evade detection. At the very least, they might confuse someone conducting forensic analysis on an infected host.

Such changes are commonly seen in malware families as they evolve over time. We can expect to see more changes with IcedID malware and the TA551 campaign during the coming months.

Finally, the run method for installer DLLs retrieved by TA551 Word macros changed during November 2020:

- Old method: `regsvr32.exe [installer DLL filename]`
- New method: `rundll32.exe [installer DLL filename],ShowDialogA -r`

However, up-to-date information is necessary to ensure proper detection for a constantly-evolving campaign like TA551.

Conclusion

TA551 has evolved since we last reviewed this threat actor [deploying Valak malware in July 2020](#). We frequently saw IcedID as follow-up malware in previous months from Valak and Ursnif infections installed by TA551. This threat actor appears to have eliminated malware downloaders like Valak and Ursnif and is now deploying IcedID directly.

Although TA551 has settled on IcedID as its malware payload, we continue to see changes in traffic patterns and infection artifacts as this campaign evolves.

Organizations with adequate spam filtering, proper system administration and up-to-date Windows hosts have a much lower risk of infection. Palo Alto Networks Next-Generation Firewall customers are further protected from this threat with the Threat Prevention security subscription, which detects the malware. AutoFocus customers can track this activity using the TA551 and IcedID tags.

Indicators of Compromise

[This GitHub repository](#) currently has more than 50 text files containing various indicators associated with TA551 from mid-July 2020-November 2020. Each text file represents a specific day the campaign was active, and it contains SHA256 hashes, document names, associated URLs and other related data, some of which we’ve also shared through our Twitter handle [@Unit42_Intel](#).

Source: <https://unit42.paloaltonetworks.com/ta551-shathak-icedid/>