Recent TZW Campaigns Revealed As Part of GlobeImposter Malware Family

sentinelone.com/blog/recent-tzw-campaigns-revealed-as-part-of-globeimposter-malware-family/

February 15, 2023

In recent years, efforts to apprehend threat groups and shrink their operating landscape have gone international. As authorities across multiple countries continue to implement sanctions and openly communicate current trends to the public, threat groups increasingly resort to rebranding or creating similar variants under different names to sidestep crackdowns and obfuscate their identities.

In a February 2023 blog post, Ahnlab described a new ransomware campaign affecting South Korean organizations which deployed a malware they dubbed “TZW” ransomware. Our research links TZW ransomware to a known malware family called GlobeImposter (sometimes referred to as LOLNEK or LOLKEK). Close inspection of host origins and prominent file similarities used in both TZW and GlobeImposter campaigns suggest that actors behind GlobeImposter are updating their payloads and obfuscating their infrastructure in a manner consistent with a rebrand effort.

FROM THE FRONT LINES
Recent TZW Campaigns Revealed As Part of GlobeImposter Malware Family
By Jim Walter
SentinelOne

Overview of GlobeImposter & New Variant TZW

GlobeImposter has a long and winding history. First observed in-the-wild in 2016, the name “GlobeImposter” is based on the ransomware’s mimicry of Globe ransomware payloads. Multiple new versions and variations of GlobeImposter have appeared in the years since. Frequently, these have been referred to by their extension (e.g., `.DREAM`, `.Nutella`, `.NARCO`, `.LEGO`). However, these are all part of the same umbrella malware family. In that same year, Emisoft released a decryption tool for early versions of GlobeImposter. Shortly after, the malware authors responded with an updated version for which no decryption tools are available.

Since 2017, campaigns delivering GlobeImposter have continued to proliferate even though the ransomware has only evolved slightly. The ransomware has also been used in conjunction with some well-documented high-end cybercriminal groups. For example, in 2017 TA505 (also known as G0092, GOLD TAHOE) began using GlobeImposter in replacement of Jaff, GandCrab, and Snatch to extend the reach and effectiveness of their campaigns.

GlobeImposter’s Delivery Methods Explained

GlobeImposter is most often delivered via phishing email as an attachment or a link to a malicious attachment. The payloads are typically distributed via 7zip or traditional zip file archives. The archives often include a JavaScript (`.js`) file that downloads and executes the GlobeImposter payload.

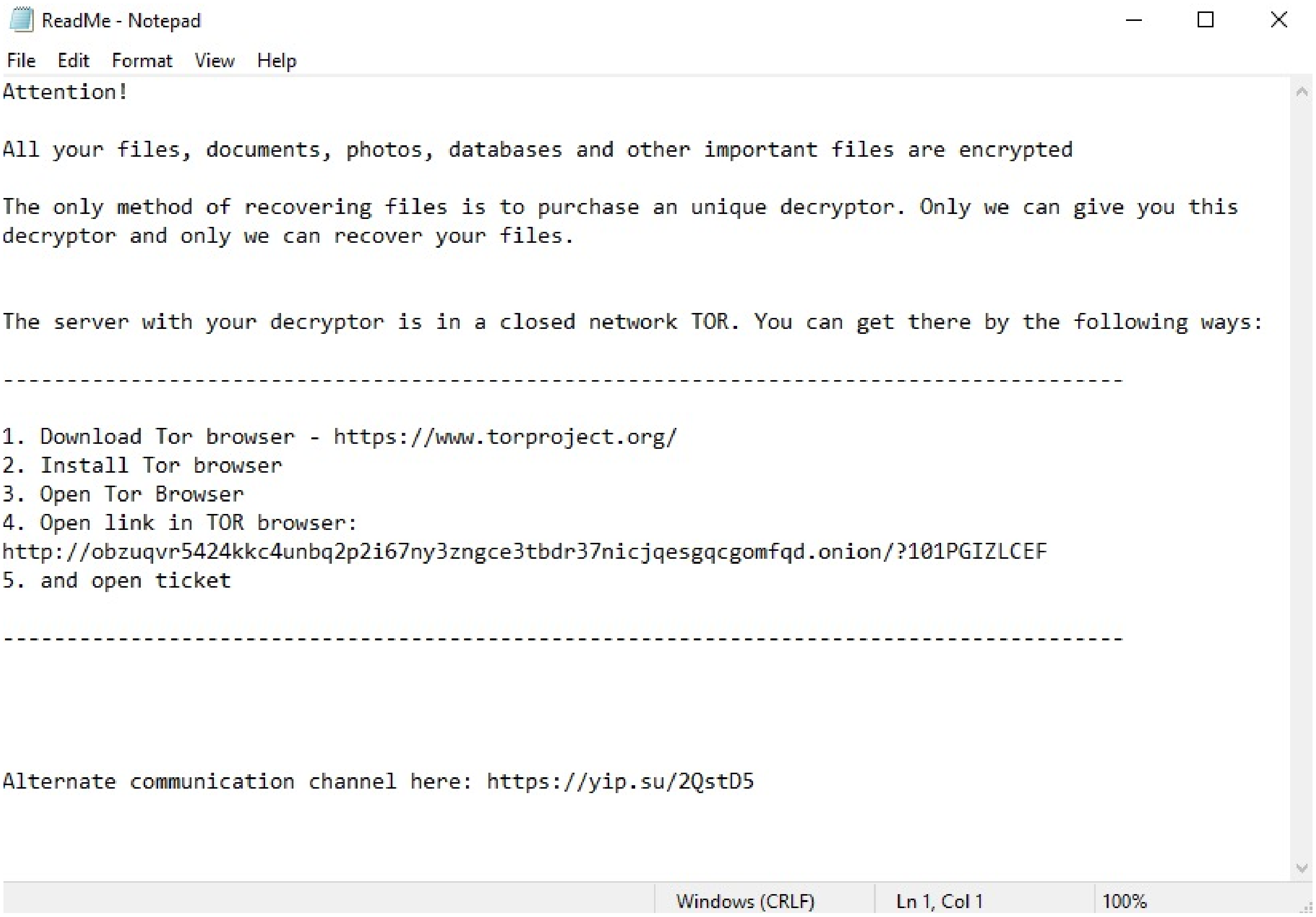
More recent campaigns from within the past three years still tend to follow this formula.

GlobeImposter has also been distributed as a later-stage infection within some well-known botnets. For example, in 2017 GlobeImposter was distributed via the Necurs botnet. This occurred as part of multiple spam campaigns that also included 7zip archives and followed the execution flow previously described.

Linking TZW Attacks to GlobeImposter

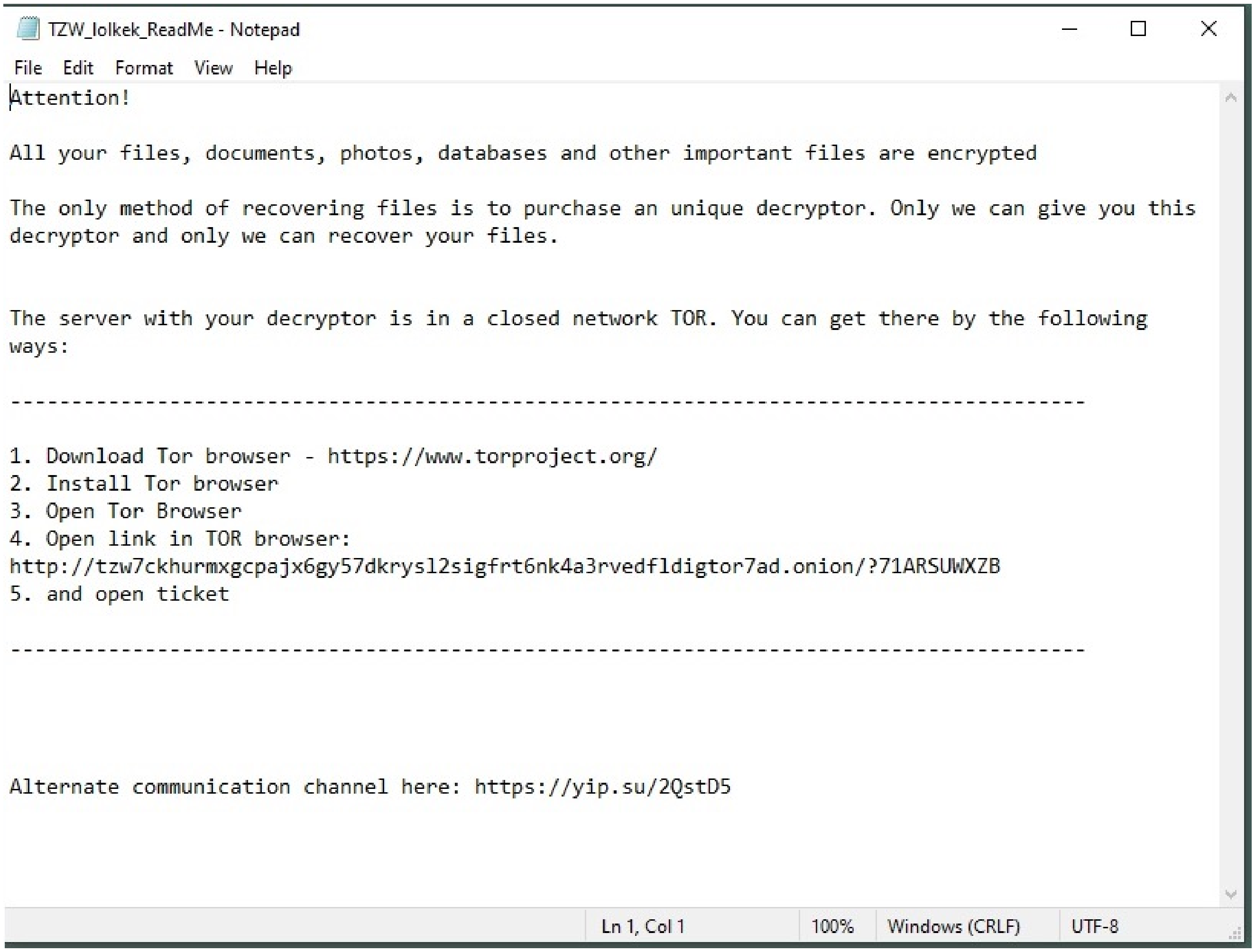
AhnLab’s research revealed a ransomware campaign they referred to as “TZW” with victims in South Korea. The name is derived from the first 3 characters of the TOR-based victim portal. A closer look suggests that “TZW” samples represent a new variant of the GlobeImposter family.

The pre-TZW GlobeImposter ransom notes follow the same template as the current TZW samples. Ransom note similarities are far from reliable, but it’s worth noting their likenesses.



```
Attention!

All your files, documents, photos, databases and other important files are encrypted

The only method of recovering files is to purchase an unique decryptor. Only we can give you this
decryptor and only we can recover your files.


The server with your decryptor is in a closed network TOR. You can get there by the following ways:

----------------------------------------------------------------------------------------

1. Download Tor browser - https://www.torproject.org/
2. Install Tor browser
3. Open Tor Browser
4. Open link in TOR browser:
http://obzuqvr5424kkc4unbq2p2i67ny3zngce3tbdr37nicjqesgqcgomfqd.onion/?101PGIZLCEF
5. and open ticket

----------------------------------------------------------------------------------------




Alternate communication channel here: https://yip.su/2QstD5
```

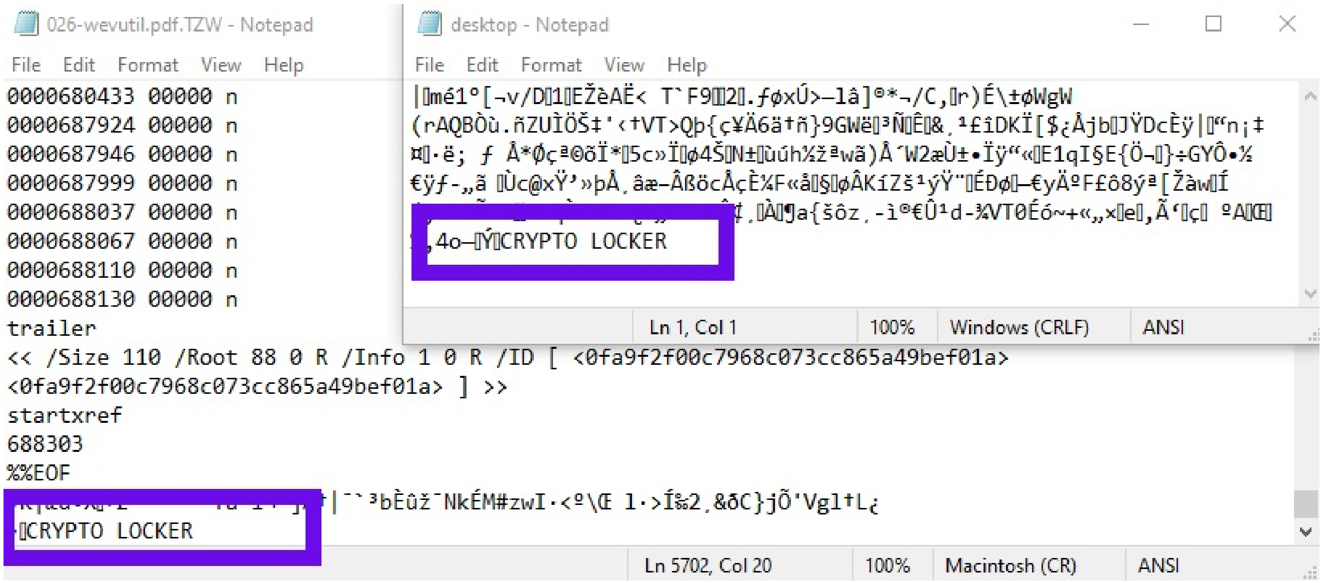
Example of a GlobeImposter ransom note.



```
Attention!

All your files, documents, photos, databases and other important files are encrypted

The only method of recovering files is to purchase an unique decryptor. Only we can give you this
decryptor and only we can recover your files.


The server with your decryptor is in a closed network TOR. You can get there by the following
ways:

----------------------------------------------------------------------------------------


1. Download Tor browser - https://www.torproject.org/
2. Install Tor browser
3. Open Tor Browser
4. Open link in TOR browser:
http://tzw7ckhurmxgcpajx6gy57dkrysl2sigfrt6nk4a3rvedfldigtor7ad.onion/?71ARSUWXZB
5. and open ticket

----------------------------------------------------------------------------------------




Alternate communication channel here: https://yip.su/2QstD5
```

Example of a TZW variant GlobeImposter ransom note.

Once a machine is infected, more concrete markers indicate a deeper level of similarity. One such marker is the “CRYPTO LOCKER” string appended to the tail of the encrypted files. This is a known marker present across GlobeImposter variants.

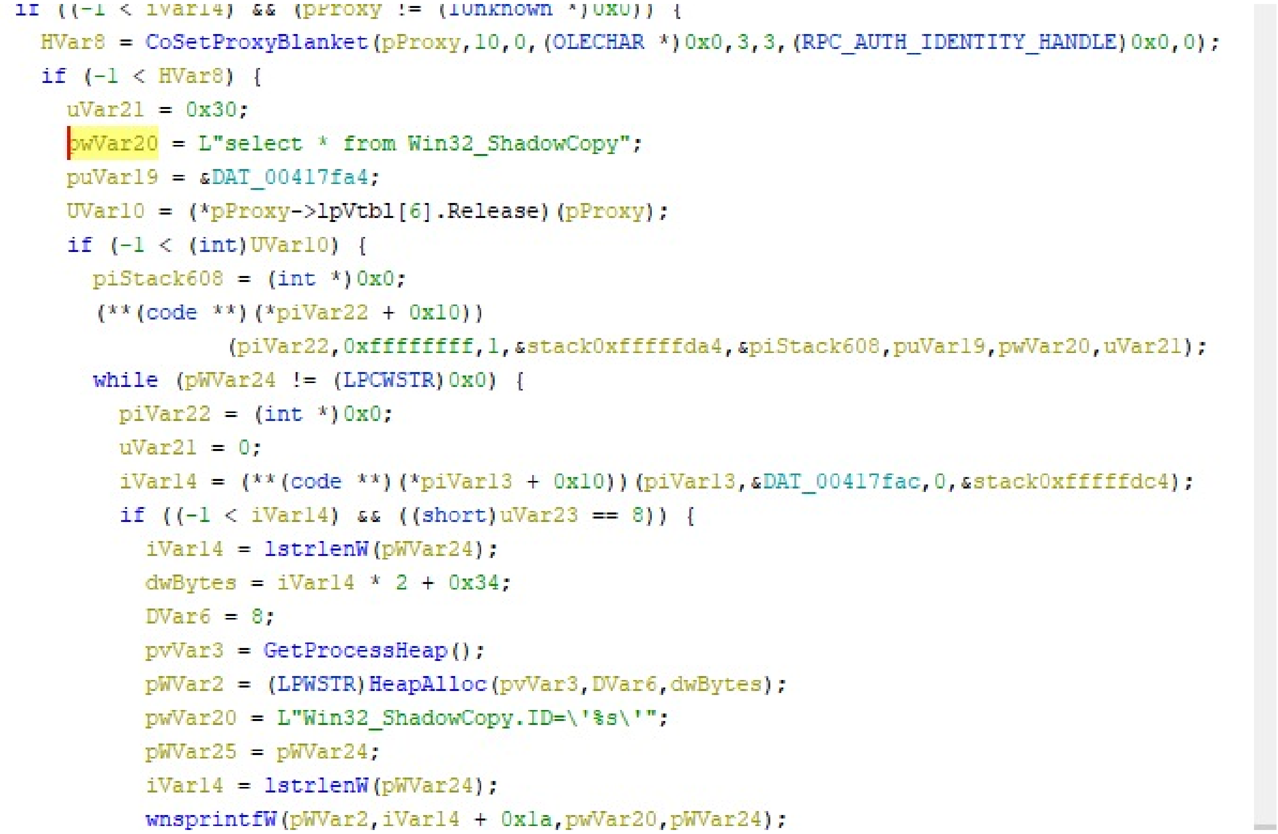


```
0000680433 00000 n
0000687924 00000 n
0000687946 00000 n
0000687999 00000 n
0000688037 00000 n
0000688067 00000 n
0000688110 00000 n
0000688130 00000 n
trailer
<< /Size 110 /Root 88 0 R /Info 1 0 R /ID [ <0fa9f2f00c7968c073cc865a49bef01a>
<0fa9f2f00c7968c073cc865a49bef01a> ] >>
startxref
688303
%%EOF
                       |¯`³bÈûž¯NkÉM#zwI·<º\Œ 1·>Í‰2¸&ðC}jÕ'Vgl†L¿
CRYPTO LOCKER
```

```
|mé1°[¬v/D1EŽèAË< T`F92.ƒøxÚ>—1â]®*¬/C,r)É\±øWgW
(rAQBÒù.ñZUÌÖŠ‡'‹†VT>Qþ{ç¥Ä6ä†ñ}9GWë³ÑÊ&¸¹£îDKÏ[$¿ÅjbJŸDcÈÿ|“n¡‡
¤·ë; ƒ Å*Øçª©õÏ*5c»Ïø4ŠN±ùúh½žªwã)Å´W2æÙ±•Ïÿ“«E1qI§E{Ö¬}÷GYÔ•½
€ÿƒ-„ã Ùc@xŸ’»þÅ¸âæ–ÂßöcÅçÈ¼F«å§øÂKíZš¹ýŸ¨ÉÐø—€yÄºF£ô8ýª[Žàwİ
                    ‡¸À¶a{šôz¸-ì®€Û¹d-¾VT0Éó~+«„xe,Ã‘ç ºAŒ
,4o—ÝCRYPTO LOCKER
```

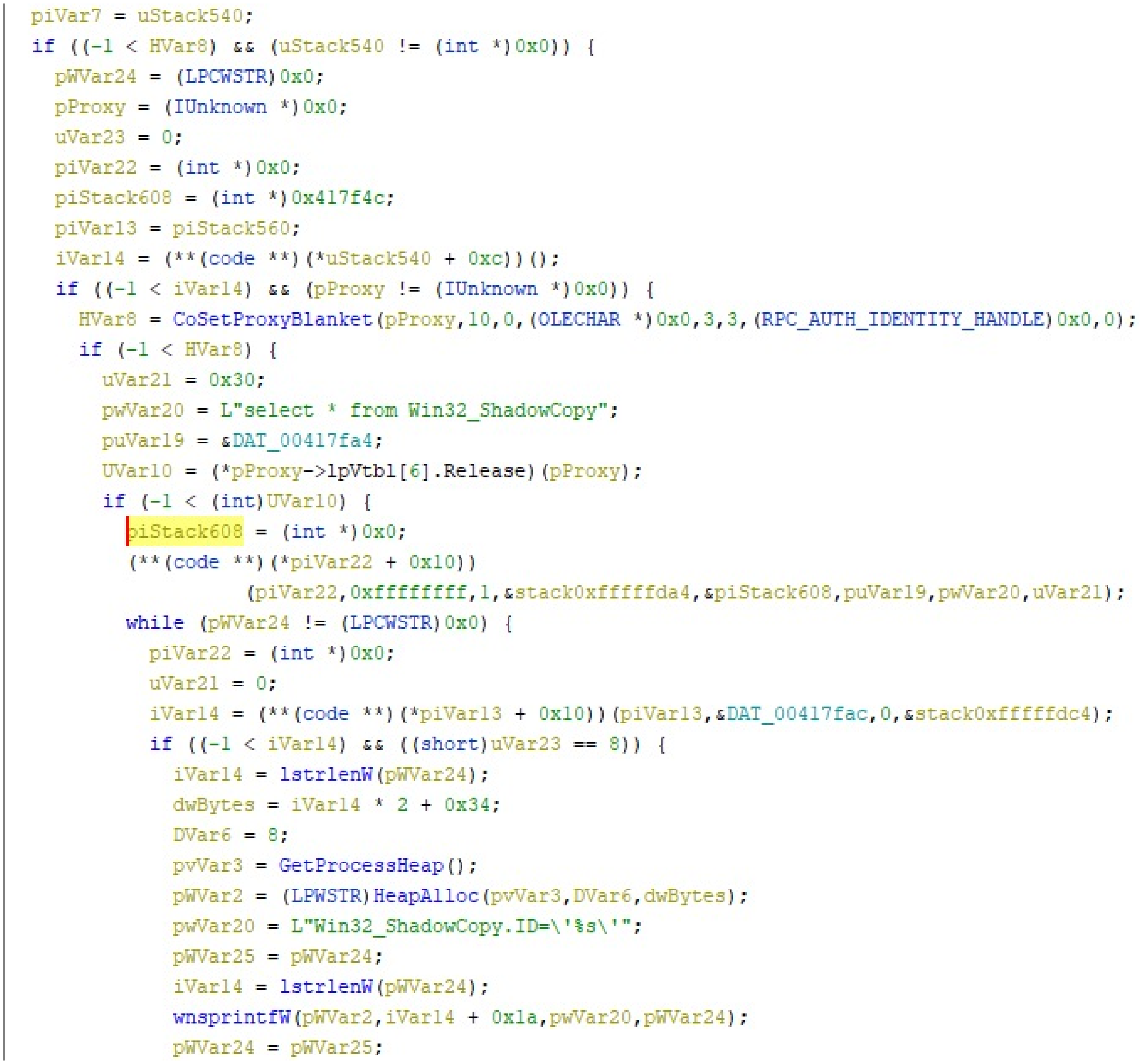
Examples of CRYPTO LOCKER markers at EOF (TZW and LOLKEK variants).

GlobeImposter has the ability to delete volume shadow copies, thereby inhibiting the recovery of data. There are clear similarities around the methodology of the VSS removal.



```
if ((-1 < iVar14) && (pProxy != (IUnknown *)0x0)) {
  HVar8 = CoSetProxyBlanket(pProxy,10,0,(OLECHAR *)0x0,3,3,(RPC_AUTH_IDENTITY_HANDLE)0x0,0);
  if (-1 < HVar8) {
    uVar21 = 0x30;
    pwVar20 = L"select * from Win32_ShadowCopy";
    puVar19 = &DAT_00417fa4;
    UVar10 = (*pProxy->lpVtbl[6].Release)(pProxy);
    if (-1 < (int)UVar10) {
      piStack608 = (int *)0x0;
      (**(code **)(*piVar22 + 0x10))
                (piVar22,0xffffffff,1,&stack0xfffffda4,&piStack608,puVar19,pwVar20,uVar21);
      while (pWVar24 != (LPCWSTR)0x0) {
        piVar22 = (int *)0x0;
        uVar21 = 0;
        iVar14 = (**(code **)(*piVar13 + 0x10))(piVar13,&DAT_00417fac,0,&stack0xfffffdc4);
        if ((-1 < iVar14) && ((short)uVar23 == 8)) {
          iVar14 = lstrlenW(pWVar24);
          dwBytes = iVar14 * 2 + 0x34;
          DVar6 = 8;
          pvVar3 = GetProcessHeap();
          pWVar2 = (LPWSTR)HeapAlloc(pvVar3,DVar6,dwBytes);
          pwVar20 = L"Win32_ShadowCopy.ID=\'%s\'";
          pWVar25 = pWVar24;
          iVar14 = lstrlenW(pWVar24);
          wnsprintfW(pWVar2,iVar14 + 0x1a,pwVar20,pWVar24);
```

GlobeImposter shadow copy removal highlights.

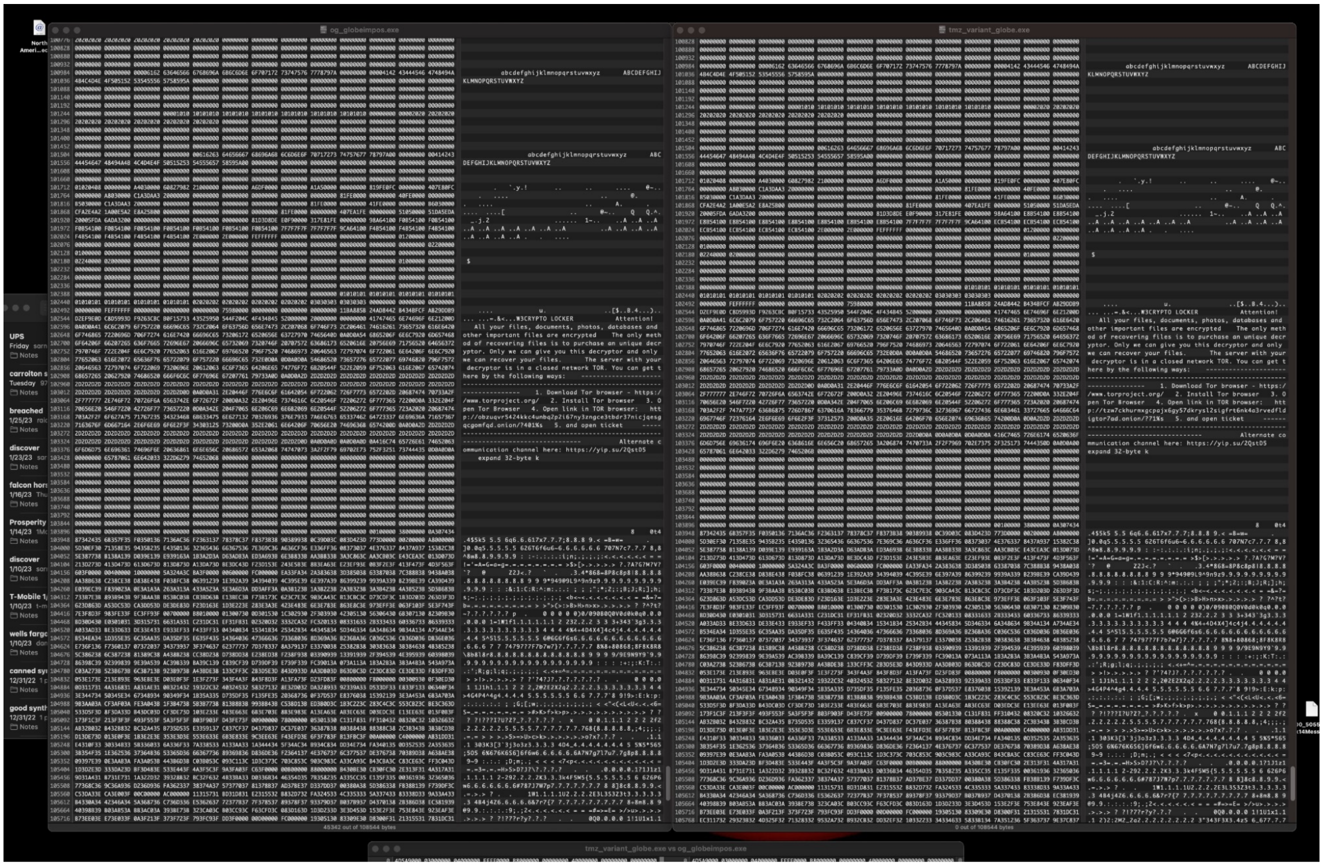


```
piVar7 = uStack540;
if ((-1 < HVar8) && (uStack540 != (int *)0x0)) {
  pWVar24 = (LPCWSTR)0x0;
  pProxy = (IUnknown *)0x0;
  uVar23 = 0;
  piVar22 = (int *)0x0;
  piStack608 = (int *)0x417f4c;
  piVar13 = piStack560;
  iVar14 = (**(code **)(*uStack540 + 0xc))();
  if ((-1 < iVar14) && (pProxy != (IUnknown *)0x0)) {
    HVar8 = CoSetProxyBlanket(pProxy,10,0,(OLECHAR *)0x0,3,3,(RPC_AUTH_IDENTITY_HANDLE)0x0,0);
    if (-1 < HVar8) {
      uVar21 = 0x30;
      pwVar20 = L"select * from Win32_ShadowCopy";
      puVar19 = &DAT_00417fa4;
      UVar10 = (*pProxy->lpVtbl[6].Release)(pProxy);
      if (-1 < (int)UVar10) {
        piStack608 = (int *)0x0;
        (**(code **)(*piVar22 + 0x10))
                  (piVar22,0xffffffff,1,&stack0xfffffda4,&piStack608,puVar19,pwVar20,uVar21);
        while (pWVar24 != (LPCWSTR)0x0) {
          piVar22 = (int *)0x0;
          uVar21 = 0;
          iVar14 = (**(code **)(*piVar13 + 0x10))(piVar13,&DAT_00417fac,0,&stack0xfffffdc4);
          if ((-1 < iVar14) && ((short)uVar23 == 8)) {
            iVar14 = lstrlenW(pWVar24);
            dwBytes = iVar14 * 2 + 0x34;
            DVar6 = 8;
            pvVar3 = GetProcessHeap();
            pWVar2 = (LPWSTR)HeapAlloc(pvVar3,DVar6,dwBytes);
            pwVar20 = L"Win32_ShadowCopy.ID=\'%s\'";
            pWVar25 = pWVar24;
            iVar14 = lstrlenW(pWVar24);
            wnsprintfW(pWVar2,iVar14 + 0x1a,pwVar20,pWVar24);
            pWVar24 = pWVar25;
```

GlobeImposter vs TZW variant shadow copy removal procedure.

Code and functionality, by and large, are identical across GlobeImposter payloads pointing to `obzuqvr5424kkc4unbq2p2i67ny3zngce3tbdr37nicjqesgqcgomfqd[.] onion` and those pointing to the newer `tzw7ckhurmxgcpajx6gy57dkrysl2sigfrt6nk4a3rvedfldigtor7ad[.]onion`.

A thorough comparison of the two respective samples shows there are only minor differences.

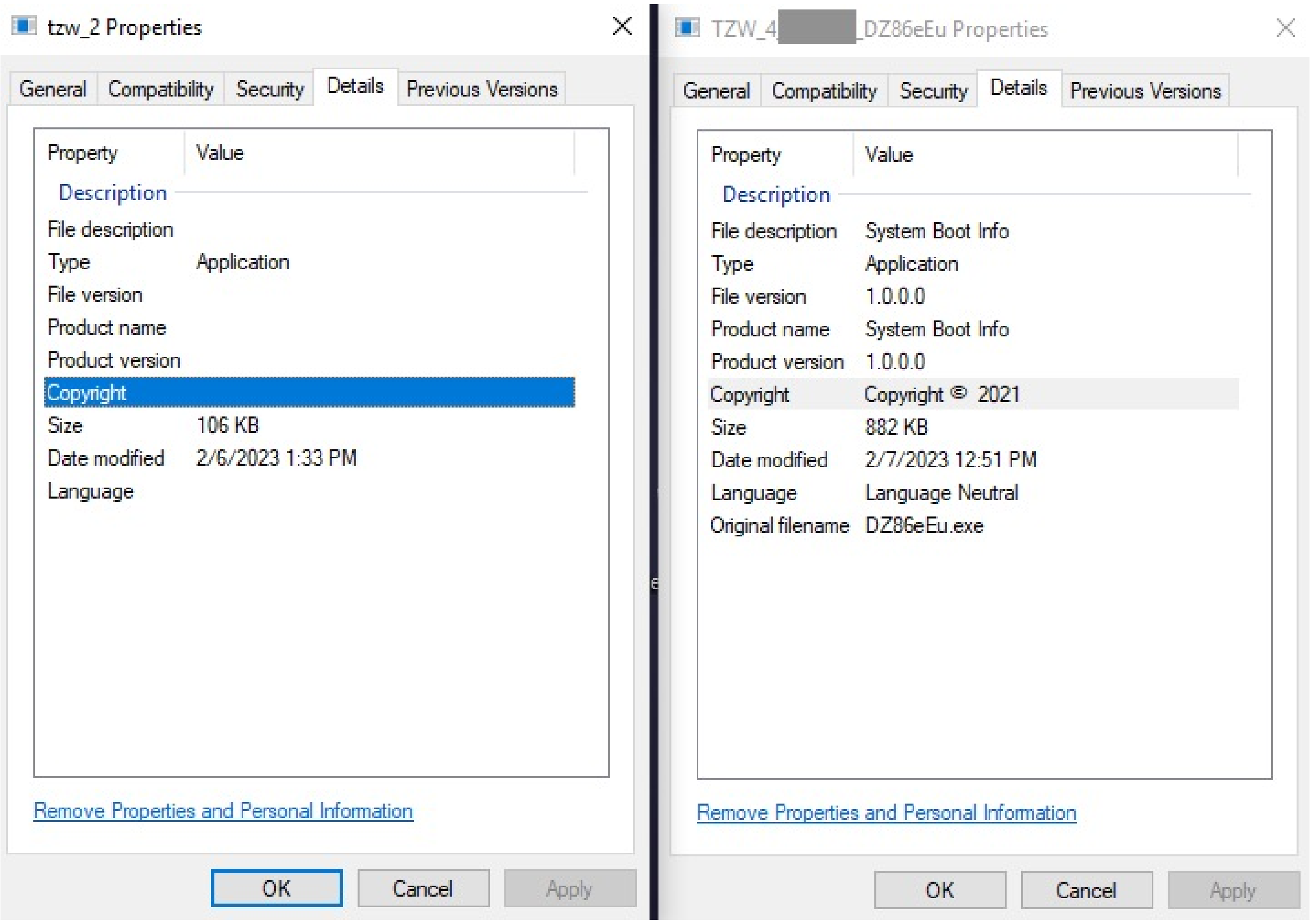


```
...  ...=.&<...W3CRYPTO LOCKER            Attention!
   All your files, documents, photos, databases and
other important files are encrypted    The only meth
od of recovering files is to purchase an unique decr
yptor. Only we can give you this decryptor and only
we can recover your files.      The server with your
 decryptor is in a closed network TOR. You can get t
here by the following ways:     --------------------
----------------------------------------------------
---------------    1. Download Tor browser - https:/
/www.torproject.org/   2. Install Tor browser   3. O
pen Tor Browser   4. Open link in TOR browser:   htt
p://obzuqvr5424kkc4unbq2p2i67ny3zngce3tbdr37nicjqesg
qcgomfqd.onion/?401%s   5. and open ticket     -----
----------------------------------------------------
------------------------------          Alternate c
ommunication channel here: https://yip.su/2QstD5
    expand 32-byte k
```

```
...  ...=.&<...W3CRYPTO LOCKER            Attention!
   All your files, documents, photos, databases and
other important files are encrypted    The only meth
od of recovering files is to purchase an unique decr
yptor. Only we can give you this decryptor and only
we can recover your files.      The server with your
 decryptor is in a closed network TOR. You can get t
here by the following ways:     --------------------
----------------------------------------------------
---------------    1. Download Tor browser - https:/
/www.torproject.org/   2. Install Tor browser   3. O
pen Tor Browser   4. Open link in TOR browser:   htt
p://tzw7ckhurmxgcpajx6gy57dkrysl2sigfrt6nk4a3rvedfld
igtor7ad.onion/?71%s   5. and open ticket     ------
----------------------------------------------------
------------------------------          Alternate co
mmunication channel here: https://yip.su/2QstD5
expand 32-byte k
```

Zoomed-out view of GlobeImposter (hex) compared against the TZW variation.

AhnLab's research describes artifacts from a specific sample within a specific campaign. We have seen the newer TZW variations vary somewhat with regards to file metadata.



Property	Value
Description	
File description	
Type	Application
File version	
Product name	
Product version	
Copyright	
Size	106 KB
Date modified	2/6/2023 1:33 PM
Language	

TZW_4[redacted]DZ86eEu Properties
General
Compatibility
Security
Details
Previous Versions
Remove Properties and Personal Information
OK
Cancel
Apply

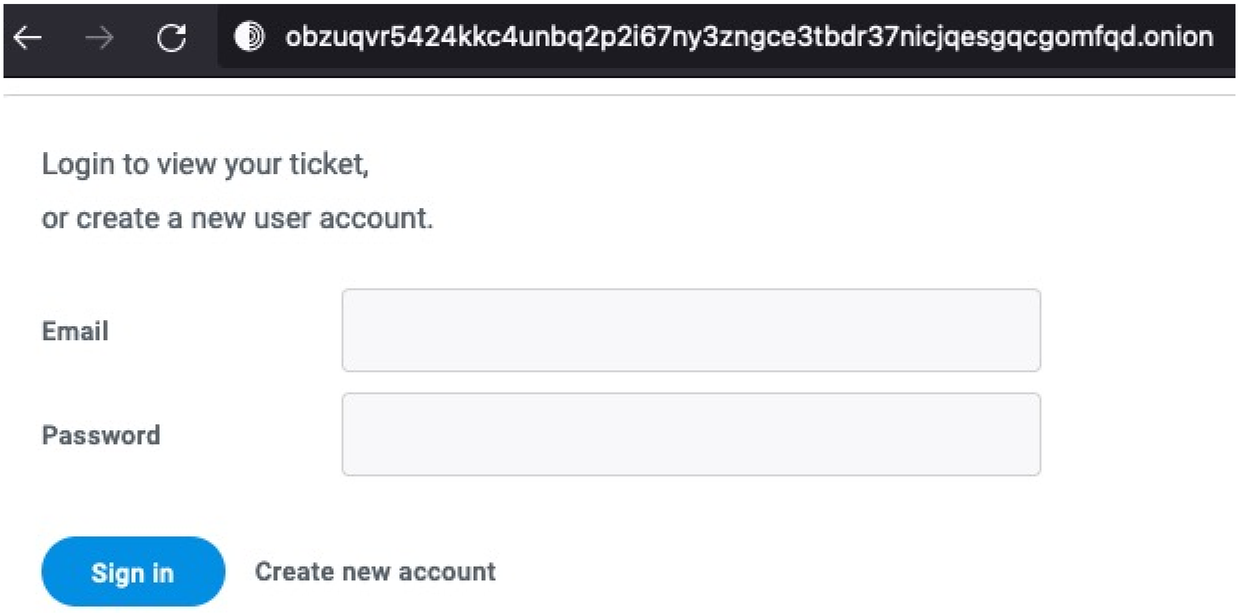
Property	Value
Description	
File description	System Boot Info
Type	Application
File version	1.0.0.0
Product name	System Boot Info
Product version	1.0.0.0
Copyright	Copyright © 2021
Size	882 KB
Date modified	2/7/2023 12:51 PM
Language	Language Neutral
Original filename	DZ86eEu.exe

Two TZW payloads, varied file metadata

A majority of the TZW variant samples that we have analyzed resemble the version on the left hand side. The version on the right was seen in the samples noted by AhnLab.

Understanding TZW and GlobeImposter's Shared Infrastructure

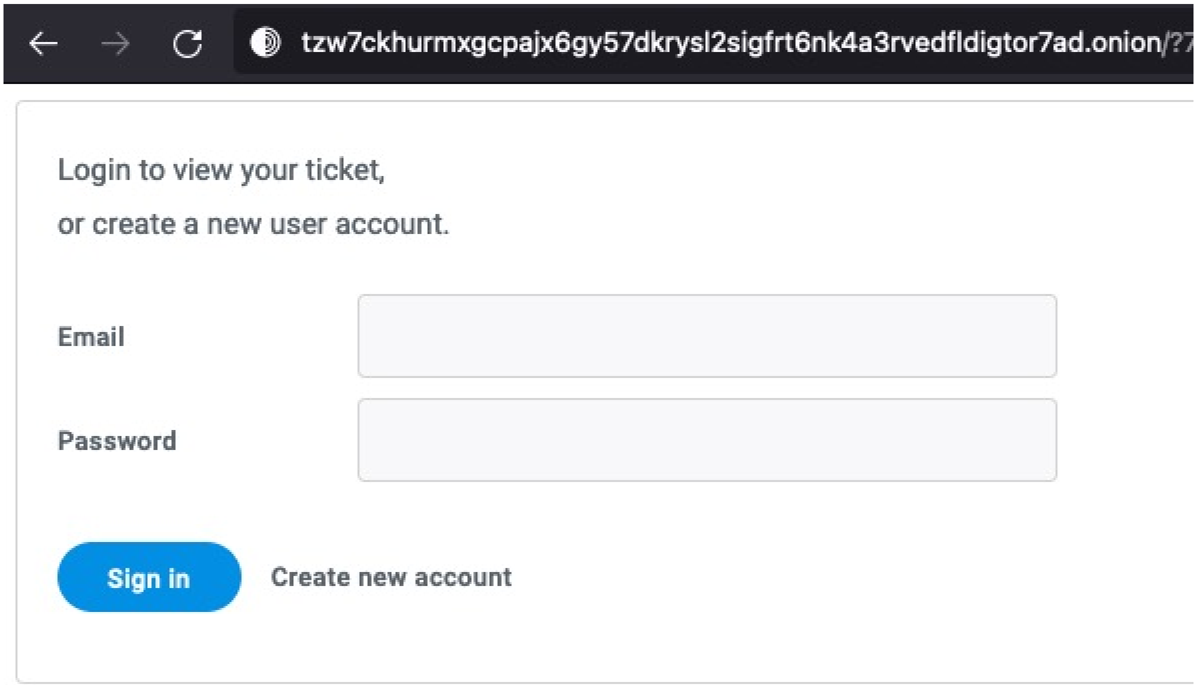
Previous GlobeImposter payloads directed victims to a TOR-based portal at `obzuqvr5424kkc4unbq2p2i67ny3zngce3tbdr37nicjqesgqcgomfqd[.]onion`.



obzuqvr5424kkc4unbq2p2i67ny3zngce3tbdr37nicjqesgqcgomfqd.onion

Login to view your ticket,
or create a new user account.

GlobeImposter Victim Portal 1.
Beginning in late 2022, we start to see victims also being directed to `tzw7ckhurmxgcpajx6gy57dkrysl2sigfrt6nk4a3rvedfldigtor7ad[.]onion`. The interfaces and required steps are identical:

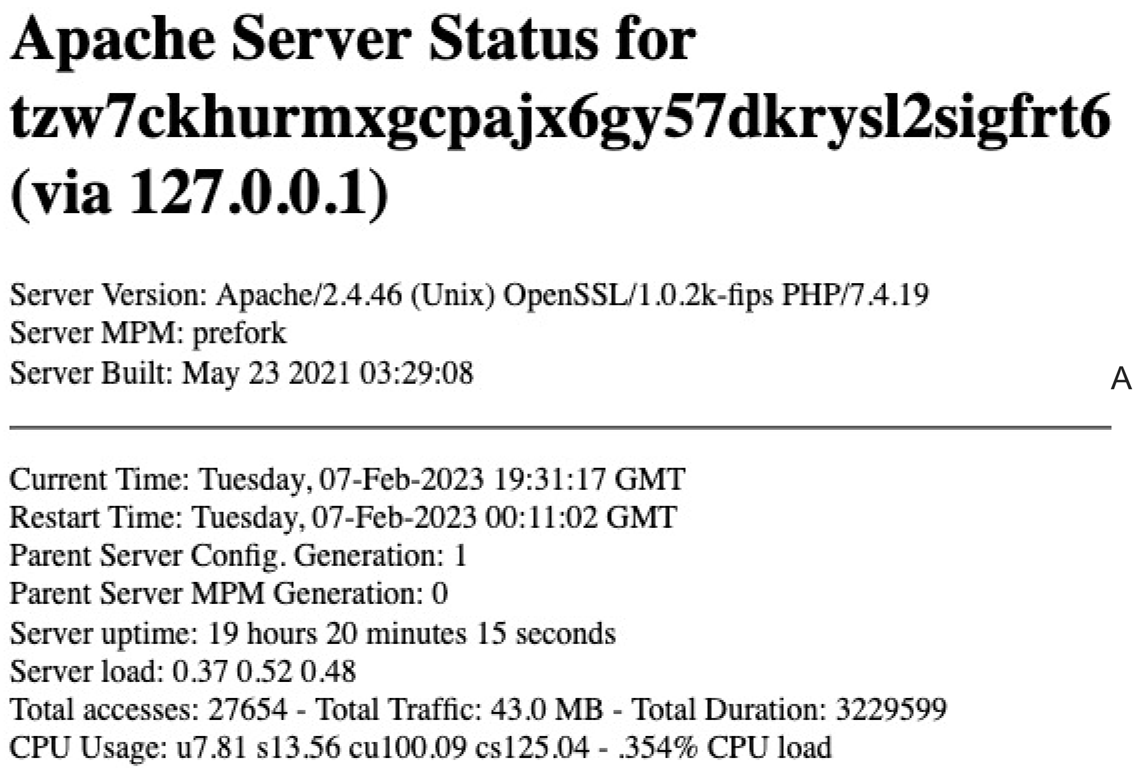


tzw7ckhurmxgcpajx6gy57dkrysl2sigfrt6nk4a3rvedfldigtor7ad.onion/?7

Login to view your ticket,
or create a new user account.

GlobeImposter Victim Portal 2 from late 2022 onward.
At the time of writing, both victim portals remain active. In addition, we can confirm the relationship between these via the publicly-viewable Apache Server Status Page.

This Apache status screen is visible as a result of a misconfiguration on the Apache server, allowing us to see all the active vhosts (virtual hosts) present there.



Apache Server Status for tzw7ckhurmxgcpajx6gy57dkrysl2sigfrt6 (via 127.0.0.1)

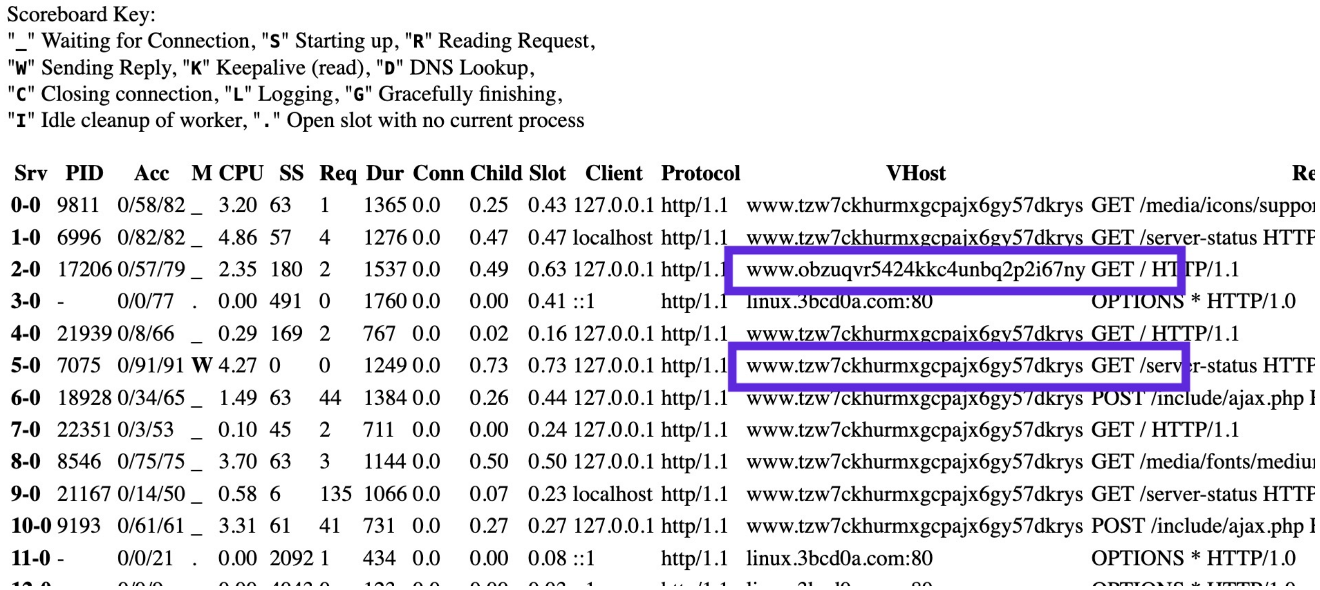
Server Version: Apache/2.4.46 (Unix) OpenSSL/1.0.2k-fips PHP/7.4.19
Server MPM: prefork
Server Built: May 23 2021 03:29:08

Current Time: Tuesday, 07-Feb-2023 19:31:17 GMT
Restart Time: Tuesday, 07-Feb-2023 00:11:02 GMT
Parent Server Config. Generation: 1
Parent Server MPM Generation: 0
Server uptime: 19 hours 20 minutes 15 seconds
Server load: 0.37 0.52 0.48
Total accesses: 27654 - Total Traffic: 43.0 MB - Total Duration: 3229599
CPU Usage: u7.81 s13.56 cu100.09 cs125.04 - .354% CPU load

Apache Status page – GlobeImposter victim portal.

Through this view we see that the following vhosts are active on the device.

```
obzuqvr5424kkc4unbq2p2i67ny3zngce3tbdr37nicjqesgqcgomfqd[.]onion
tzw7ckhurmxgcpajx6gy57dkrysl2sigfrt6nk4a3rvedfldigtor7ad[.]onion
linux[.]3bcd0a[.]com
```



Scoreboard Key:
"_" Waiting for Connection, "S" Starting up, "R" Reading Request,
"W" Sending Reply, "K" Keepalive (read), "D" DNS Lookup,
"C" Closing connection, "L" Logging, "G" Gracefully finishing,
"I" Idle cleanup of worker, "." Open slot with no current process

Srv	PID	Acc	M	CPU	SS	Req	Dur	Conn	Child	Slot	Client	Protocol	VHost	Re
0-0	9811	0/58/82	_	3.20	63	1	1365	0.0	0.25	0.43	127.0.0.1	http/1.1	www.tzw7ckhurmxgcpajx6gy57dkrys	GET /media/icons/suppo
1-0	6996	0/82/82	_	4.86	57	4	1276	0.0	0.47	0.47	localhost	http/1.1	www.tzw7ckhurmxgcpajx6gy57dkrys	GET /server-status HTTP
2-0	17206	0/57/79	_	2.35	180	2	1537	0.0	0.49	0.63	127.0.0.1	http/1.1	www.obzuqvr5424kkc4unbq2p2i67ny	GET / HTTP/1.1
3-0	-	0/0/77	.	0.00	491	0	1760	0.0	0.00	0.41	::1	http/1.1	linux.3bcd0a.com:80	OPTIONS * HTTP/1.0
4-0	21939	0/8/66	_	0.29	169	2	767	0.0	0.02	0.16	127.0.0.1	http/1.1	www.tzw7ckhurmxgcpajx6gy57dkrys	GET / HTTP/1.1
5-0	7075	0/91/91	W	4.27	0	0	1249	0.0	0.73	0.73	127.0.0.1	http/1.1	www.tzw7ckhurmxgcpajx6gy57dkrys	GET /server-status HTTP
6-0	18928	0/34/65	_	1.49	63	44	1384	0.0	0.26	0.44	127.0.0.1	http/1.1	www.tzw7ckhurmxgcpajx6gy57dkrys	POST /include/ajax.php
7-0	22351	0/3/53	_	0.10	45	2	711	0.0	0.00	0.24	127.0.0.1	http/1.1	www.tzw7ckhurmxgcpajx6gy57dkrys	GET / HTTP/1.1
8-0	8546	0/75/75	_	3.70	63	3	1144	0.0	0.50	0.50	127.0.0.1	http/1.1	www.tzw7ckhurmxgcpajx6gy57dkrys	GET /media/fonts/mediu
9-0	21167	0/14/50	_	0.58	6	135	1066	0.0	0.07	0.23	localhost	http/1.1	www.tzw7ckhurmxgcpajx6gy57dkrys	GET /server-status HTTP
10-0	9193	0/61/61	_	3.31	61	41	731	0.0	0.27	0.27	127.0.0.1	http/1.1	www.tzw7ckhurmxgcpajx6gy57dkrys	POST /include/ajax.php
11-0	-	0/0/21	.	0.00	2092	1	434	0.0	0.00	0.08	::1	http/1.1	linux.3bcd0a.com:80	OPTIONS * HTTP/1.0

Vhosts on GlobeImposter victim portal.

This evidence of shared infrastructure suggests that the newly rebranded TZW ransomware samples are likely being operated by the same group that was pushing recent waves of GlobeImposter malware.

How to Protect Against GlobeImposter and TZW Ransomware

SentinelOne Singularity™ protects against malicious behaviors and malware associated with GlobeImposter and TZW.

With the site policy set to Protect, GlobeImposter ransomware is detected and prevented automatically. In Detect-only mode, analysts can observe the malware's behaviour and file encryption attempts, rolling back the device to a clean state on completion of the test.

Watch Video At:

https://youtu.be/QrNSunn3Wu8

Conclusion

Based on our analysis, the TZW ransomware recently documented by AhnLab is yet another example of the threat actors behind GlobeImposter pivoting their TTPs alongside a rebrand, including a new but related Onion address. We also show that the old "LOLNEK" Onion address and the Onion address within the TZW variant are hosted on the same server as two vhosts.

Regardless of the name or brand, GlobeImposter continues to pose a threat to enterprises. Ensuring good user hygiene, along with strong, properly-configured, and robust security controls will go a long way to prevent these attacks from affecting your environment.

SentinelOne Singularity™ protects against malicious behaviors and malware associated with GlobeImposter and TZW.

Watch Video At:

https://youtu.be/QrNSunn3Wu8

Indicators of Compromise

SHA1

4585da0ff7a763be1a46d78134624f7cd13e6940
14be1c43fbfb325858cda78a126528f82cf77ad2
dc98b516c9c589c2b40bc754732ad5f16deb7c82
d034880d1233d579854e17b6ffad67a18fb33923
858f3f7f656397fcf43ac5ea13d6d4cbe7a5ca11
9a080cd497b8aa0006dc953bd9891155210c609c
8c64e820a4c5075c47c4fbaea4022dc05b3fd10b
3326708ba36393b1b4812aa8c88a03d72689ac24
cf5ab37612f24ed422a85e3745b681945c96190e
cf21028b54c4d60d4e775bf05efa85656de43b68

Onions

tzw7ckhurmxgcpajx6gy57dkrysl2sigfrt6nk4a3rvedfldigtor7ad[.]onion
obzuqvr5424kkc4unbq2p2i67ny3zngce3tbdr37nicjqesgqcgomfqd[.]onion

MITRE ATT&CK

T1005 – Data from Local System
T1202 – Indirect Command Execution
T1486 – Data Encrypted for Impact

T1070.004 – Indicator Removal: File Deletion
T1112 – Modify Registry
T1012 – Query Registry
T1083 – File and Directory Discovery
T1027.002 – Obfuscated Files or Information: Software Packing
T1082 – System Information Discovery
T1490 – Inhibit System Recovery
T1547.001 – Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder