Trend Micro Incorporated
Research Paper
2013

FAKEM RAT

Malware Disguised as Windows® Messenger and Yahoo!® Messenger

By: Nart Villeneuve
Jessa dela Torre

Contents

Introduction

The perpetrators of targeted attacks aim to maintain persistent presence in a target network in order to extract sensitive data when needed. To maintain persistent presence, attackers seek to blend in with normal network traffic and use ports that are typically allowed by firewalls. As a result, many of the malware used in targeted attacks utilize the HTTP and HTTPS protocols to appear like web traffic. However, while these malware do give attackers full control over a compromised system, they are often simple and configured to carry out a few commands.

Attackers often use remote access Trojans (RATs), which typically have graphical user interfaces (GUIs) and remote desktop features that include directory browsing, file transfer, and the ability to take screenshots and activate the microphone and web camera of a compromised computer. Attackers often use publicly available RATs like Gh0st, PoisonIvy, Hupigon, and DRAT, and "closed-released" RATs like MFC Hunter and PlugX.[1] However, the network traffic these RATs produce is well-known and easily detectable although attackers still successfully use them.[2]

Attackers always look for ways to blend their malicious traffic with legitimate traffic to avoid detection. We found a family of RATs that we call "FAKEM" that make their network traffic look like various protocols. Some variants attempt to disguise network traffic to look like Windows® Messenger and Yahoo!® Messenger traffic. Another variant tries to make the content of its traffic look like HTML. While the disguises the RATs use are simple and distinguishable from legitimate traffic, they may be just good enough to avoid further scrutiny.

1 Gh0st: http://download01.norman.no/documents/ThemanyfacesofGh0stRat.pdf and http://www.mcafee.com/ca/resources/white-papers/foundstone/wp-know-your-digital-enemy.pdf; PoisonIvy: https://media.blackhat.com/bh-eu-10/presentations/Dereszowski/BlackHat-EU-2010-Dereszowski-Targeted-Attacks-slides.pdf; Hupigon: http://www.f-secure.com/v-descs/backdoor_w32_hupigon.shtml; DRAT: http://blog.trendmicro.com/trendlabs-security-intelligence/watering-holes-and-zero-day-attacks/; MFC Hunter: http://blog.trendmicro.com/trendlabs-security-intelligence/japan-us-defense-industries-among-targeted-entities-in-latest-attack/; and PlugX: http://about-threats.trendmicro.com/us/webattack/112/Pulling+the+Plug+on+PlugX

2 http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-detecting-apt-activity-with-network-traffic-analysis.pdf

All three versions of the FAKEM RAT that we investigated were distributed via spear-phishing emails using social engineering to lure targets into executing a malicious attachment. While we observed the use of different themes, the content of the emails were always interesting to potential targets.

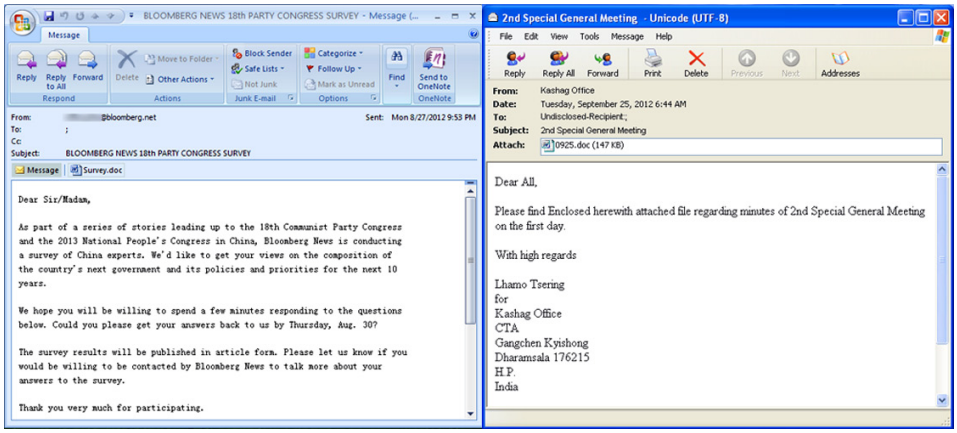


FIGURE 1: Sample spear-phishing emails with attachments that drop FAKEM RAT

The malicious attachments were most often Microsoft® Word® documents with code that exploits the following vulnerabilities:

- **CVE-2010-3333:** RTF Stack Buffer Overflow Vulnerability addressed in Microsoft Security Bulletin MS10-087.[3]
- **CVE-2012-0158:** MSCOMCTL.OCX RCE Vulnerability addressed in Microsoft Security Bulletin MS12-027.[4]

We also found a Microsoft® Excel® file that exploits CVE-2009-3129, the Excel Featheader Record Memory Corruption Vulnerability addressed in Microsoft Security Bulletin MS09-067.[5] We also saw samples that were simply executable (.EXE) files.

3 http://technet.microsoft.com/en-us/security/bulletin/MS10-087
4 http://technet.microsoft.com/en-us/security/bulletin/ms12-027
5 http://technet.microsoft.com/en-us/security/bulletin/MS09-067

Installation

After exploitation, an .EXE file packed with UPX is dropped.[6] After initially dropping the malicious file named **hkcmd.exe** to the **%Temp% folder**, the malware typically copies itself using the name, **tpframe.exe**, to the **%System%** folder.

It then adds the following registry entry to enable its automatic execution at every system startup:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Windows\CurrentVersion\policies\Explorer\run
tpbar = "%System%\tpframe.exe"
```

Backdoor

The network traffic the malware produces is designed to look like Windows Messenger traffic. Malware of this type were discussed on Twitter, noted by SonicWALL, and found to have been active as far back as September 2009.[7] However, it remains unclear if all the attacks that used this malware were connected.

The malicious traffic begins with headers similar to actual Windows Messenger traffic:

```
MSG 5 N 130
MIME-Version: 1.0
```

However, beyond this, you will see that the traffic is not valid Windows Messenger traffic but may be sufficiently disguised as such to escape further scrutiny.

6 UPX is a free tool that compresses executable files. However, it is commonly used to pack malware files, see http://upx.sourceforge.net/ for more details.

7 https://twitter.com/mikko/status/232851667446538241, https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=464, and https://twitter.com/diocyde/statuses/232873023651336192

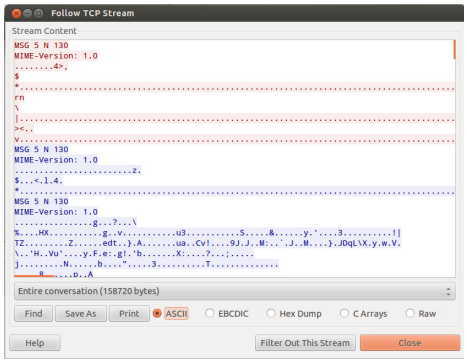


FIGURE 2: Malicious traffic disguised as legitimate Windows Messenger traffic

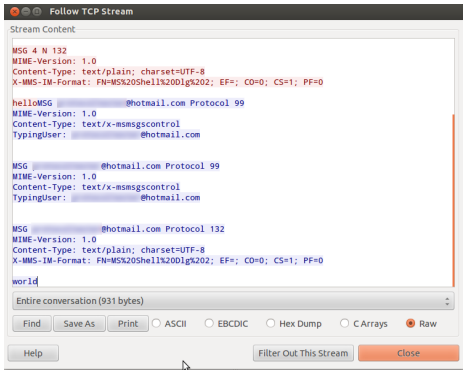


FIGURE 3: Legitimate Windows Messenger traffic

Compared with actual Windows Messenger traffic shown in Figure 3, it is easy to distinguish the malicious traffic shown in Figure 2.

During our investigation of the fake "Windows Messenger" RAT, we found another version that attempts to disguise its network traffic as Yahoo! Messenger traffic. The network communication this version uses begins with **YMSG**, the Yahoo! Messenger traffic header.

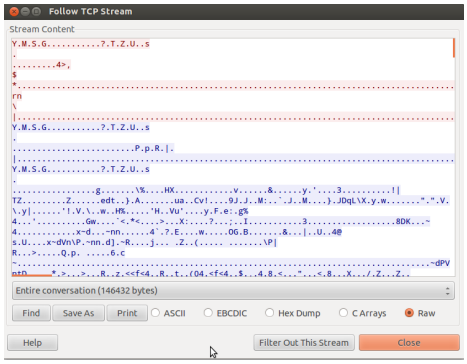


FIGURE 4: Malicious traffic disguised as Yahoo! Messenger traffic

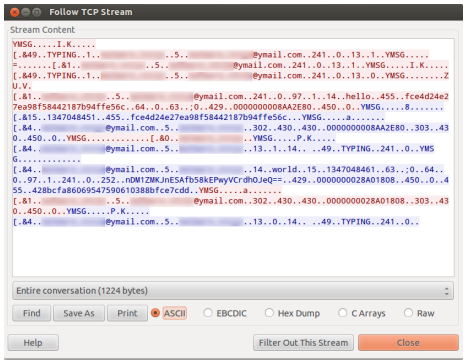


FIGURE 5: Legitimate Yahoo! Messenger traffic

However, the network traffic shown in Figure 4 does not resemble legitimate Yahoo! Messenger traffic beyond the use of the header, **YMSG**. Compared with the legitimate Yahoo! Messenger traffic shown in Figure 5, it is easy to distinguish between the two.

A third version of the FAKEM RAT attempts to disguise the network traffic it produces as HTML. The malicious traffic begins with strings like **<html><title>1..56</title><body>** or **<html><title>12356</title><body>**.[8]

8 This variant was referenced during an incident documented by AlienVault in March 2012 in http://labs.alienvault.com/labs/index.php/2012/alienvault-research-used-as-lure-in-targeted-attacks/.

This is a fairly rudimentary disguise and odd because you would expect HTML to be the result of a request to a web server and not as something a client would send to a web server.

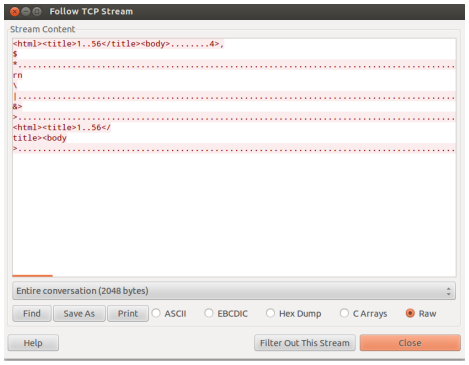


FIGURE 6: Malicious traffic disguised as HTML traffic

Network Traffic Encryption

The network communication between the compromised computer and the RAT controller is encrypted. The encryption is the same across variants and done at the bit level. Each byte is XOR-ed by every letter in the string, **YHCRA**, and rotated 3 bits to the right after every XOR operation. Encrypting the communication ensures that the suspicious data passed between the compromised host and the attackers cannot be easily viewed in plain text. The communication comes in 1024-byte blobs of data that start with the 32-byte header. It appears that attackers may specify any kind of fake headers within the first 32 bytes in order to disguise the subsequent network traffic.

The following bits of information are initially sent by the compromised host when the communication starts:

- User name
- Computer name
- OEM code page identifier
- What looks like a campaign code but only for some samples

The commands are not preconfigured as the malware relies on the data sent by the server. For instance, when a client receives the command, **0211**, this signifies that it should execute the accompanying data in memory.

The following are the commands the server issues and their meanings:

- **0211:** Execute code.
- **0212:** Reconnect to receive data.
- **0213:** Sleep, close socket, and reconnect.
- **0214:** Exit.

To determine the RAT's capabilities, we allowed the attackers to infiltrate a honeypot computer and captured all of the network traffic it generated. We decrypted the network traffic and determined the commands the attackers used, which include:

- **CmdMana:** Command Manager allows attackers to execute shell commands.
- **FileMan:** File Manager allows the attackers to browse directories.
- **HostIn:** Host Information provides information about the compromised computer.
- **ProcMan:** Process Manager gives attackers access to running processes.
- **RegMana:** Registry Manager gives attackers access to the Windows registry.
- **Scree:** Screen takes a snapshot of the desktop.
- **ServiceMa:** Service Manager allows access to services.
- **Passwo:** Password accesses stored passwords like those saved in Internet Explorer (IE).
- **UStea:** Uploads files from a compromised computer.

The Windows Messenger samples we analyzed were clustered into five groups that did not have overlapping linkages. Four of the clusters were relatively small and focused on four different domains:

- vcvcvcvc.dyndns.org
- zjhao.dtdns.net
- avira.suroot.com
- *.googmail.com

The **vcvcvcvc.dyndns.org** domain is particularly interesting because we also found it being used as a command-and-control (C&C) server for Protux—a well-known malware family that has been used in many targeted attacks over the years. We also found that the **avira.suroot.com** domain used as a C&C server for yet another malware family we call "cxgid."

The ***.googmail.com** domain was slightly larger and included names like **apple12.crabdance.com** and **apple12.co.cc**. However, the largest cluster revolved around the ***.yourturbe.org** domain and overlapped with the HTML variant. We also found small clusters of the HTML variant that revolved around the domain, **endless.zapto.org**, which was downloaded as a second-stage malware by Protux.

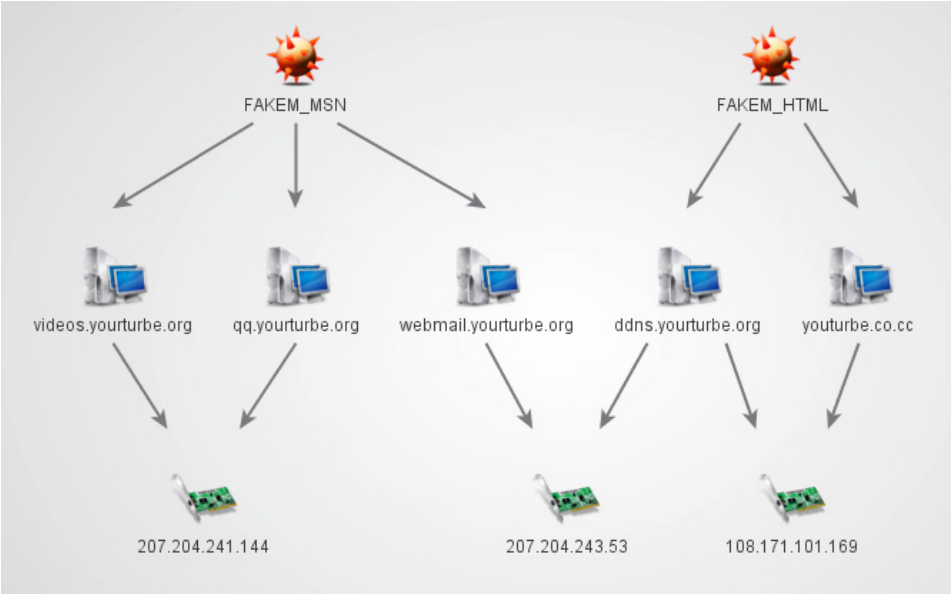


FIGURE 7: FAKEM domains associated with the Windows Messenger and HTML variants

Meanwhile, the Yahoo! Messenger samples we analyzed all accessed **freeavg.sytes.net**—a domain name that frequently resolved to different IP addresses.

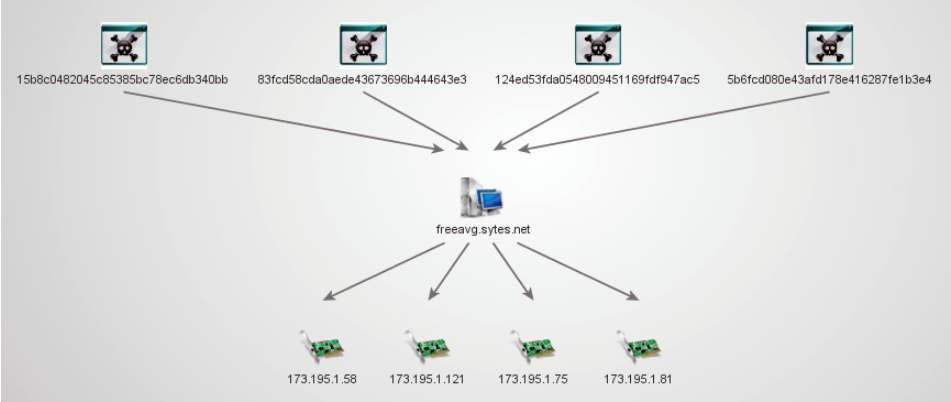


FIGURE 8: FAKEM domains associated with the Yahoo! Messenger variant

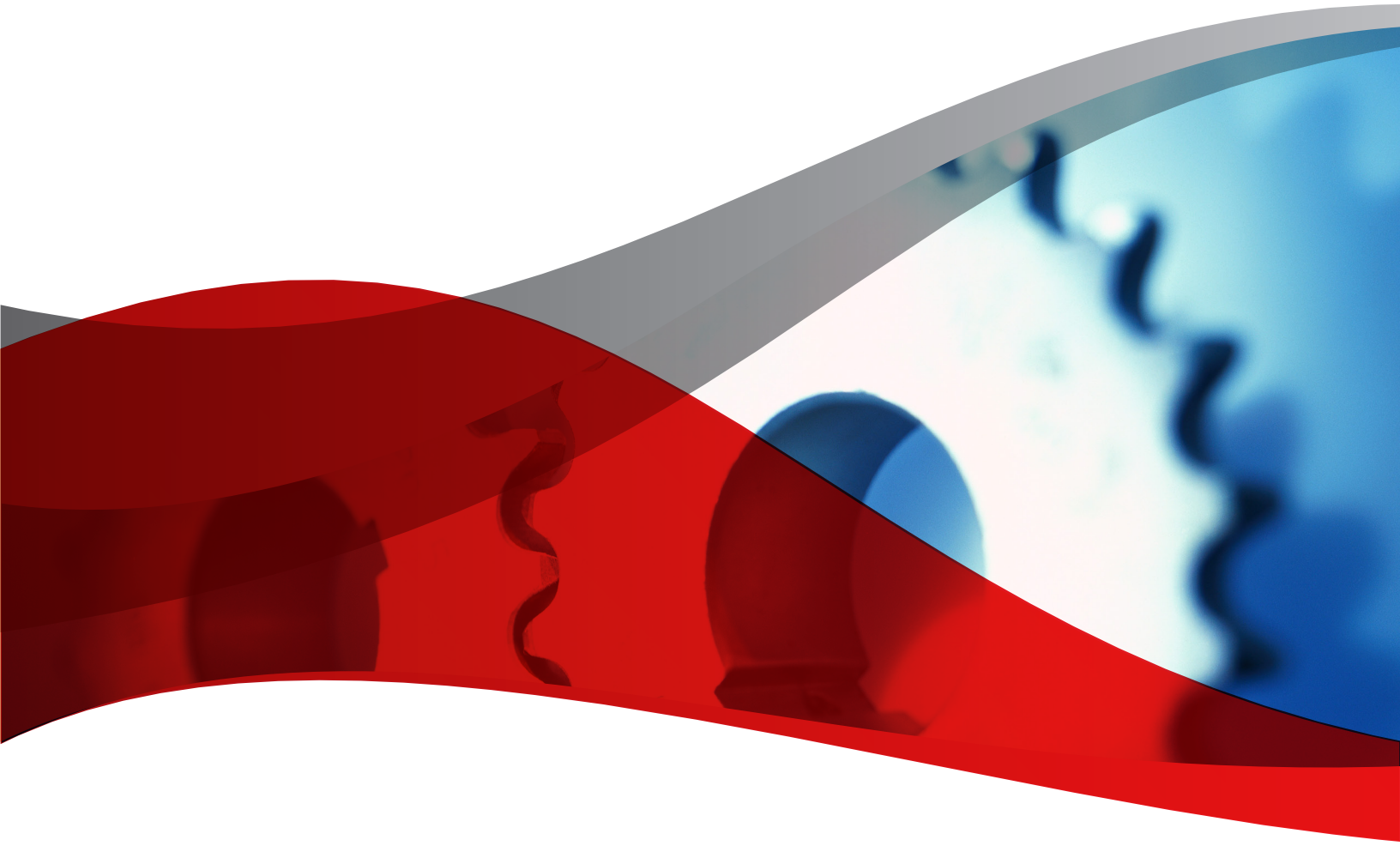
The various samples we collected appear to belong to groups that overlapped a little. This suggests that rather than being associated with a particular campaign, the use of various FAKEM RATs could be distributed among multiple threat actors.

Conclusion

Knowledge of the attack tools, techniques, and infrastructure of adversaries is critical for developing defensive strategies. This research paper examined three variants of a RAT—FAKEM—that attempt to disguise the network traffic they produce to stay under the radar.

Now that popular RATs like GhOst and PoisonIvy have become well-known and can easily be detected, attackers are looking for methods to blend in with legitimate traffic. While it is possible to distinguish the network traffic FAKEM RAT variants produce for the legitimate protocols they aim to spoof, doing so in the context of a large network may not be not easy. The RAT's ability to mask the traffic it produces may be enough to provide attackers enough cover to survive longer in a compromised environment.

Fortunately, solutions like Trend Micro™ Deep Discovery can help network administrators protect their organizations from attacks that use the FAKEM RAT by detecting the traffic its variants produce.



TREND MICRO INCORPORATED

Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years' experience, we deliver top-ranked client, server and cloud-based security that fits our customers' and partners' needs, stops new threats faster, and protects data in physical, virtualized and cloud environments. Powered by the industry-leading Trend Micro™ Smart Protection Network™ cloud computing security infrastructure, our products and services stop threats where they emerge—from the Internet. They are supported by 1,000+ threat intelligence experts around the globe.

TREND MICRO INCORPORATED

10101 N. De Anza Blvd.
Cupertino, CA 95014

U.S. toll free: 1 +800.228.5651
Phone: 1 +408.257.1500
Fax: 1 +408.257.2003

www.trendmicro.com

TREND MICRO™

Securing Your Journey to the Cloud