FireEye™

Supply Chain Analysis: From Quartermaster to Sunshop

FireEye Labs
Authors: Ned Moran,
James T. Bennett

Contents

Executive Summary

Many seemingly unrelated cyber attacks may, in fact, be part of a broader offensive fueled by a shared development and logistics infrastructure—a finding that suggests some targets are facing a more organized menace than they realize.

This report examines 11 advanced persistent threat (APT) campaigns targeting a wide swath of industries. Though they appeared unrelated at first, further investigation uncovered several key links between them: the same malware tools, the same elements of code, binaries with the same timestamps, and signed binaries with the same digital certificates.

Taken together, these commonalities point to centralized APT planning and development. How prevalent this model has become is unclear. But adopting it makes financial sense for attackers, so the findings may imply a bigger trend.

This report focuses on two key findings:

- Shared development and logistics
- A shared malware-builder tool

Shared development and logistics

Examining the 11 APT campaigns revealed a shared development and logistics operation used to support several APT actors in distinct but overlapping campaigns. This development and logistics operation is best described as a "digital quartermaster." Its mission: supply and maintain malware tools and weapons to support cyber espionage. This digital quartermaster also might be a cyber arms dealer of sorts, a common supplier of tools used to conduct attacks and establish footholds in targeted systems.

Shared builder tool

FireEye researchers located a builder tool likely used in some of the 11 APT campaigns. The tools appear to be written in Chinese, and the testing infrastructure appears to all be configured with the native Chinese language character set, and the dialogues and menu options in the builder tool are in Chinese.

The Sunshop connection

In May 2013, FireEye first reported on the "Sunshop" campaign, which compromised several strategic websites and redirected visitors to a site serving multiple exploits.[1] In August 2013, FireEye reported that the campaign was continuing[2] and, later that month, discovered additional related attacks.

Examining the underlying infrastructure of these attacks revealed that the campaign utilized resources shared across other APT campaigns not initially tied to Sunshop.

The other campaigns included multiyear onslaughts targeting companies across 15 industries. Given the wide range of targets observed, the campaigns' specific objectives (beyond the obvious intellectual property theft) are unclear.

1 Ned Moran. "Ready for Summer: The Sunshop Campaign." May 2013.

2 Ibid. "The Sunshop Campaign Continues." August 2013.

This report outlines the following:

- The quantity and categories of malicious binaries related to the originally identified Sunshop attacks and 10 other campaigns subsequently linked to Sunshop
- The underlying infrastructure, including components of code used across these campaigns
- Clusters of APT activity previously believed to be unrelated
- A malware builder that likely supported one of these APT activity clusters

Targeted industries

The 11 interconnected campaigns targeted these industries:

- Aerospace/Defense/Airlines
- Applied research and development
- Chemicals/Manufacturing/Mining
- Higher education
- Entertainment/Media/Hospitality
- Energy/Utilities/Petroleum refining
- Financial services
- Federal government
- State and local government
- Healthcare/Pharmaceuticals
- High-tech
- Insurance
- Legal services
- Services/Consulting/VAR
- Telecommunications

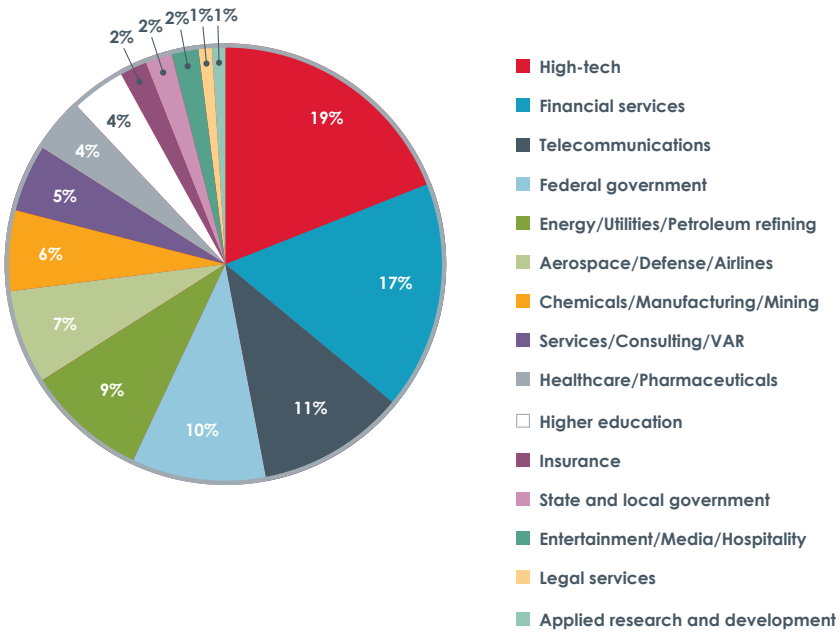

Figure 1: Percent of APT campaigns per industry

FireEye detected activity from the campaigns between July 2011 and September 2013, but they were likely active before then. Though the campaigns utilized varying techniques, tactics, and procedures (TTPs), they all leveraged a common development infrastructure. They shared (in various combinations) the following:

- Portable executable resources
- Digital certificates
- API import tables
- Compile times
- Command-and-control (CnC) infrastructure

Based on the evidence, this report outlines the following possible conclusions:

- **[High Confidence] A "Sunshop Digital Quartermaster" (SDQ) exists and supports separate APT campaigns.** FireEye believes that the most likely explanation for these links is a shared development and logistics operation that supports several APT campaigns as part of formal offensive apparatus.
- **[Low Confidence] SDQ and APT campaigns are a single actor.** Another conceivable possibility is that the 11 clusters of activity, previously believed to be independent campaigns run by different actors, are in fact one cluster of activity run by one well-resourced actor. However, we believe this scenario is less likely because each cluster of activity utilized malware samples with different artifacts such as passwords, campaign identifiers, and mutexes. These artifacts were generally consistent within each cluster of activity but differed across clusters.
- **[Medium Confidence] SDQ does not exist, and APT actors informally share among each other.** Alternatively, different actors may be responsible for the documented 11 clusters of activity. Instead of relying on a centralized development and logistics operation, they share TTPs through formal or informal channels.

Introduction

On May 20, 2013 FireEye first reported on the Sunshop campaign.[3] The actor responsible for this campaign compromised a number of strategic websites, redirecting visitors to a site serving multiple exploits. Almost three months later, FireEye reported that the campaign was continuing.[4] We discovered additional related attacks about a week after that. During the intervening time, we examined the underlying infrastructure supporting these attacks and found that the Sunshop campaign utilized resources shared across a number of other APT campaigns not initially tied to Sunshop.

What we initially believed to be 11 different APT campaigns used the same malware tools, the same elements of code, binaries with the same timestamps, and signed binaries with the same digital certificates. Through this discovery, we believe that we have identified a shared development and logistics operation used to support a number of different APT actors engaged in distinctive but overlapping campaigns. This development and logistics operation is best described as a digital quartermaster whose mission is to supply and maintain malware tools and weapons used in support of cyber espionage operations. This digital quartermaster is a possible cyber arms dealer, supplying the operators responsible for conducting attacks and establishing footholds within targeted organizations. As such, we refer to this entity as the Sunshop Digital Quartermaster (SDQ).

To support this conclusion, we first present an overview of our research, including the total number and type of malicious binaries we found to be related to Sunshop and the 10 other linked campaigns. We then describe the underlying infrastructure, including the components of code used across these campaigns. We further describe the different clusters of APT activity that we previously believed to be unrelated. Finally, we describe one of the malware builders we believe was used to support one of these clusters of APT activity.

3 Ned Moran. "Ready for Summer: The Sunshop Campaign." May 2013.

4 Ibid. "The Sunshop Campaign Continues." August 2013.

Overview

We collected 110 unique binaries, which were detected as Trojan.APT.9002, Trojan.APT.PoisonIvy, Trojan.APT.Gh0st, Trojan.APT.Kaba, and Trojan.APT.Briba. Sixty-five of these binaries were packaged with two unique manifest resources, and 47 were signed with six different digital certificates. The binaries connected to 54 unique fully qualified domains.

Detection	Number of Samples
Trojan.APT.9002	70
Trojan.APT.PoisonIvy	26
Trojan.APT.Gh0st	12
Trojan.APT.Kaba	1
Trojan.APT.Briba	1

Table 1: APT malware samples linked to the SDQ

We identified these samples by searching binaries packaged with the two unique portable executable (PE) resources that we had previously identified. We believe that these PE resources are unique to Sunshop and the 10 other linked campaigns.

We also searched for samples signed with the six different digital certificates that were used to sign binaries connected to these campaigns. These certificates were not unique to these campaigns and have been used to sign unrelated malware. Therefore, we cross-checked samples signed with any of these certificates to ensure that they were, in fact, related to the 10 campaigns we identified as linked to Sunshop.

As we identified related campaigns that leveraged the unique PE resources or digital certificates, we then pivoted off the CnC infrastructure to identify additional samples. We cross-checked samples identified through this process to ensure that they did indeed share the code elements that we previously identified as unique to Sunshop and its associated campaigns.

We searched our internal repositories, including the FireEye high performance cluster and other well-known external repositories. We primarily relied on running active searches with YARA signatures designed to identify samples, with either the PE resources or digital certificates. We also compared the import tables used in each sample to establish additional links between the 10 different campaigns linked to Sunshop.

All of this research led us to the above-mentioned 110 binaries. Figure 2 plots the samples in a Maltego chart.

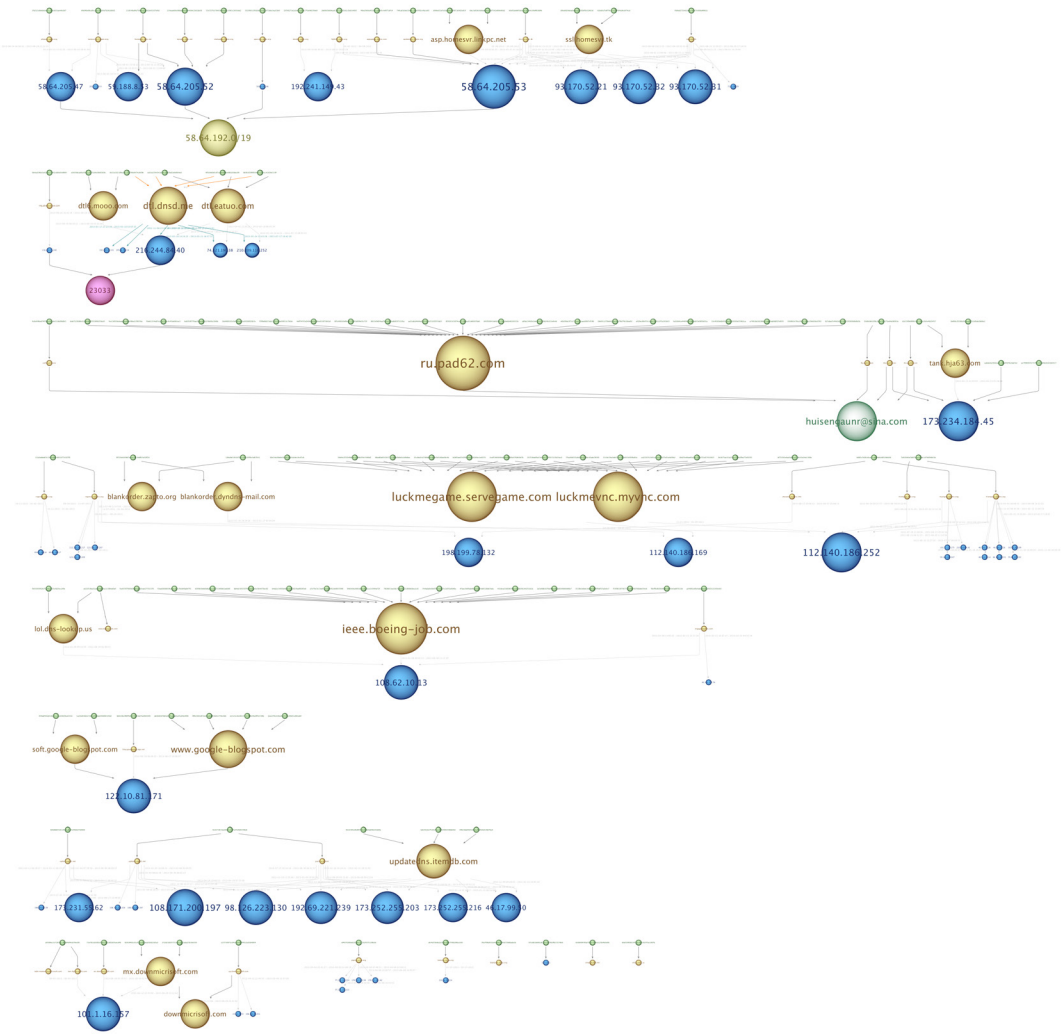

Figure 2. Eleven seemingly different APT campaigns

Figure 2 shows only domains, IP addresses, and MD5 malware/dropper hashes collected during our research. These limited data points display 11 different and seemingly independent clusters of activity.

We continued our analysis by adding the following additional data points to our graph.

- Two portable executable (PE) resources used by 64 samples in our collection
- Six different digital certificates used by 47 samples in our collections
- Hashes of the different import tables used by the binaries in our graph

These additional data points linked the 11 different clusters of activity and revealed what we believe to be a shared development logistics infrastructure.

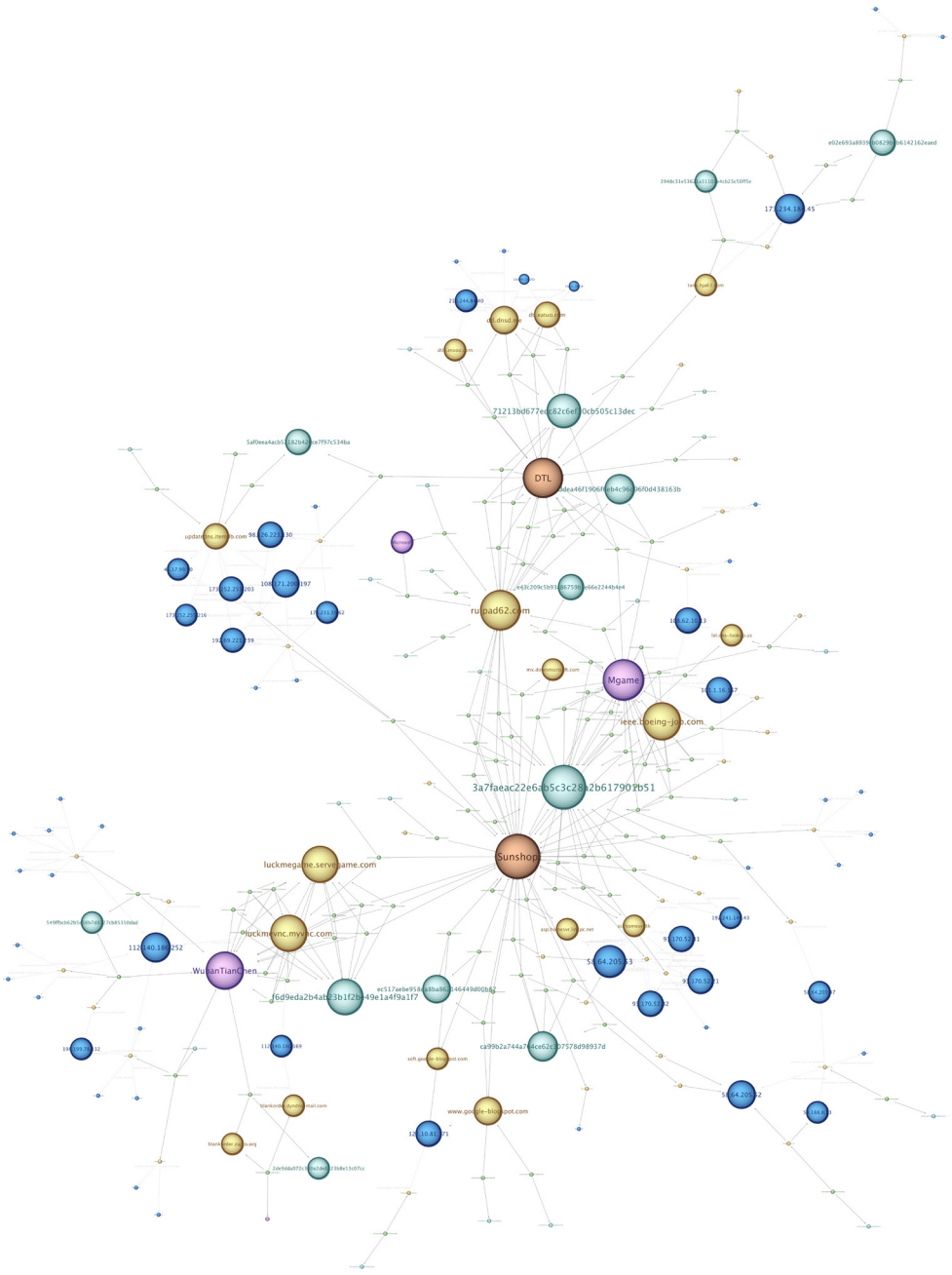

Figure 3: Eleven APT campaigns linked to the SDQ

Figure 3 illustrates the overlaps and connections that exist between what initially appeared to be 11 independent campaigns. This chart shows how the additional data points of the shared PE resources, commonly used digital certificates, and identical import tables can link these different campaigns together.

Cluster Analysis Techniques

Our research analyzed the following to identify and tie all 11 campaigns to the SDQ:

- PE resources
- Import tables
- Authenticode/Digital certificates
- Compile times

PE resource

We found that 64 of the 110 samples analyzed during this analysis were packaged with two almost identical portable executable resources. In both cases, the resources appeared to be manifests generated by the Nullsoft scriptable installation system (NSIS). Nullsoft is a script-driven tool that simplifies the installation routines of executable files onto the Microsoft Windows operating system.

Sunshop manifest

We identify the first of these manifest resources as the "Sunshop manifest." It has these properties:

```
MD5         f9e2887828846b3d383bdf9d0fded5e3
SHA256      82a98c88d3dd57a6ebc0fe7167a86875ed52ebddc6374ad640407
            efec01b1393
```

The full text of the PE resource manifest is shown in Figure 4.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
<assemblyIdentity version="1.0.0.0" processorArchitecture="X86"
name="Nullsoft.NSIS.exehead" type="win32"/>
<description>Nullsoft Install System v2.34</description>
     <dependency><dependentAssembly>
          <assemblyIdentity type="win32" name="Microsoft.Windows.Common-
          Controls" version="6.0.0.0" processorArchitecture="X86" publicKey
          Token="6595b64144ccf1df" language="*" />
     </dependentAssembly>
</dependency>
<trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
<security>
     <requestedPrivileges>
     <requestedExecutionLevel level="asInvoker" uiAccess="false"/>
     </requestedPrivileges>
</security>
</trustInfo>
</assembly>
```

Figure 4: Sunshop PE resource manifest

We found 44 unique binaries packaged with the above Sunshop manifest. These samples were detected as Trojan.APT.9002, Trojan.APT.Gh0st, and Trojan.APT.PoisonIvy. We observed these 44 samples used in eight of the 11 different campaigns discussed below.

DTL manifest

We identify the second manifest resource as the "DTL manifest." This resource has these properties:

```
MD5         010e5a583d74850cdc0655f22c7a9003
SHA256      46b966331d883d642293f4b1faa55f4c8c30b4238df8f121278
            a3752609a2cef
```

The full text of the PE resource manifest is as follows:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
<assemblyIdentity version="1.0.0.0" processorArchitecture="X86"
name="Nullsoft.NSIS.exehead" type="win32"/>
<description>Nullsoft Install System v2.34</description>
     <dependency><dependentAssembly>
          <assemblyIdentity type="win32" name="Microsoft.Windows.Common-
          Controls" version="6.0.0.0" processorArchitecture="X86" publicKey
          Token="6595b64144ccf1df" language="*" />
     </dependentAssembly>
</dependency>
<trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
     <security>
          <requestedPrivileges>
          <requestedExecutionLevel level="asInvoker" uiAccess="false"/>
          </requestedPrivileges>
     </security>
</trustInfo>
</assembly>
```

Figure 5: DTL PE resource manifest

We found 20 samples using the DTL manifest. These binaries were detected as Trojan.APT.9002. We observed these 20 samples used in five of the 11 different campaigns discussed below.

The only difference between these manifest resources is the indentation of the <*security*> elements. Lines 10 through 13 in Figure 6 detail this difference.

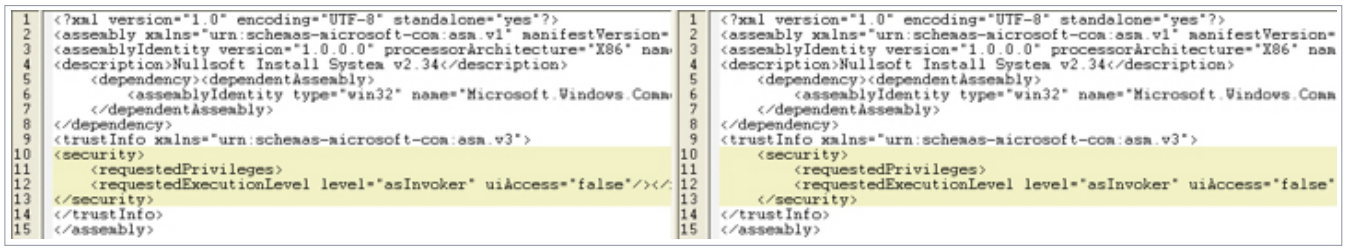

Figure 6. Comparison of Sunshop (left) and DTL (right) PE resource manifests

This slight difference results in a different hash for the resource. The similarity between these two manifests would likely go unnoticed by automated analysis. Also, the XML is improperly formatted, hinting that it was formatted manually. As an experiment, we used NSIS v2.34 to create our own simple installer and found that the XML in the manifest had no new-line or tab characters.

Import tables

We utilized a simple technique to identify similarities in import tables between the 110 different samples we analyzed during our analysis. We aggregated the import calls found in each sample and used this as a unique fingerprint. We then used these fingerprints to cluster similar samples together.

The Python code in Figure 6 relies on the module pefile and can be used to dump all the import calls used in a specific binary. The output can then be easily hashed.

```
pe = pefile.PE(file)
    for entry in pe.DIRECTORY_ENTRY_IMPORT:
        for imp in entry.imports:
            if imp.name != None:
                print entry.dll, imp.name, hex(imp.address)
            else:
                print entry.dll, hex(imp.address)
```

Figure 7: Python code to dump all import calls used in a specific binary

We found 33 unique import tables used for the 110 different samples we collected during our research. The most common import table seen had a MD5 hash of `3a7faeac22e6ab5c3c28a2b617901b51` and appeared in 38 different binaries. This particular import table appeared in both Trojan.APT.9002 and Trojan.APT.PoisonIvy binaries. It was used in eight of the 11 different clusters of activity we studied during this analysis. In addition to the identical import tables, these samples have the same code base, differing in the unpacking routine for the actual payload, indicating that they are general-purpose launchers.

Upon execution, the malware samples with the import table hash of `3a7faeac22e6ab5c3c28a2b617901b51` called back to these domains and IP addresses:

- `ieee.boeing-job[.]com`
- `lol.dns-lookup[.]us`
- `twn.ftpmicrosoft[.]com`
- `127.0.0.1`
- `piping.no-ip[.]org`
- `wv.downmicrisoft[.]com`
- `mx.downmicrisoft[.]com`
- `update1.mysq1[.]net`
- `ru.pad62[.]com`
- `phpweb.zapto[.]org`
- `asp.homesvr.linkpc[.]net`
- `dns.homesvr[.]tk`
- `ssl.homesvr[.]tk`

The second most common import table had a MD5 hash of `f6d9eda2b4ab23b1f2be49e1a4f9a1f7` and appeared in 12 different samples. These 12 samples were all detected as Trojan.APT.PoisonIvy and appeared in only one of the 10 campaigns discussed below. Upon execution, all of the malware samples with this import table hash beaconed to these domains:

- `luckmegame.servegame[.]com`
- `luckmevnc.myvnc[.]com`

The third most common import table had a MD5 hash of `71213bd677edc82c6ef30cb505c13dec` and appeared in nine different samples. These samples were all detected as Trojan.APT.9002 and appeared in three of the 10 campaigns we analyzed. Upon execution, these samples called back to these domains:

- `engage.intelfox[.]com`
- `ru.pad62[.]com`
- `tank.hja63[.]com`
- `dtl.eatuo[.]com`
- `dtl6.mooo[.]com`
- `dtl.dnsd[.]me`

Authenticode/digital certificates analysis

Digital certificates are used to validate the authenticity of code. Attackers often use stolen or spoofed digital certificates to sign their malicious code and improve the likelihood that their code will execute successfully on its target.

During our research, we found six digital certificates used to sign 44 different malware samples. These certificates are currently revoked or expired and were signed by `Microsoft`, `Sinacom`, `Facesun.cn`, `Mgame Corp`, `Guangzhou YuanLuo Technology Co., Ltd.`, and `Wuhan Tian Chen Information Technology Co., Ltd`. The full details of these certificates are available in Appendix A. According to Kaspersky, the `Mgame Corp.` and `Guangzhou YuanLuo Technology Co., Ltd.` certificates were stolen.[5] Whether the remaining certificates were also stolen—or were ever valid—is unclear.

The certificates from `Mgame Corp` and `Wuhan Tian Chen Information Technology Co. ,Ltd.` were used most frequently. We found 24 samples signed with the certificate from `Mgame Corp`. These samples were all detected as Trojan.APT.9002 and appeared in four of the 10 campaigns we studied during this research.

We found 15 samples signed with the certificate from `Wuhan Tian Chen Information Technology Co., Ltd.` These samples were all detected as Trojan.APT.PoisonIvy and appeared in one of the 10 campaigns discussed below.

Compile times

Although the compilation time of binaries can be easily forged, analyzing them is still useful. The timestamp may not reveal when a binary was actually compiled, but it can be used to cluster samples by identical compile times.

The most common compile time was December 19, 2012 at 20:25. We found 28 binaries compiled at this time. All of these binaries were detected as Trojan.APT.9002 and utilized the Sunshop PE resource. We observed samples with this timestamp in six of the 11 clusters of APT activity we studied during this research.

The next most common compile time was July 21, 2012 at 14:50. We identified five samples compiled at this time. All of these samples were detected as Trojan.APT.9002 and utilized the DTL PE resource. These samples appeared in two of the 11 campaigns.

The use of this same compile times across a number of different campaigns is another indication that a common development and logistics infrastructure supported these disparate operations.

5 Securelist. "Winnti FAQ. More than just a game." April 2013.

Clusters

The shared characteristics were used across malware tools used in at least 11 different clusters of APT activity. These clusters were originally believed to be separate and distinct campaigns and were grouped together based on shared CnC infrastructure using passive DNS data or registration information.

Cluster 1: Sunshop

The Sunshop campaign appears to primarily leverage strategic Web compromise as a vector of attack. We have detailed the specifics of the Sunshop campaign on the FireEye blog.[6] We found 15 different samples linked to the Sunshop campaign. These samples were detected as Trojan.APT.Gh0st, Trojan.APT.PoisonIvy, Trojan.APT.Briba, and Trojan.APT.9002. All of the Sunshop samples that we identified had compile times between January 1, 2013 and August 24, 2013. Twelve of the 15 utilized the Sunshop PE resource, and none was signed with any of the six identified digital certificates.

When executed, the Sunshop samples beaconed to these CnC servers:

- `appupdate.myvnc[.]com`
- `asp.homesvr.linkpc[.]net`
- `dns.homesvr[.]tk`
- `9ijhh45.zapto[.]org`
- `newtibet[.]tk`
- `ssl.homesvr[.]tk`
- `nameserver1.zapto[.]org`
- `phpweb.zapto[.]org`
- `homeweb.sytes[.]net`
- `intelupdate.hopto[.]org`
- `ajaxcode.zapto[.]org`
- `updateinfor.hopto[.]org`
- `mynews.sytes[.]net`

The campaign targeted these industries:

- State and local government
- Telecommunications
- Legal services

Table 2 outlines Sunshop-related malware and compile times.

6 See http://www.fireeye.com/blog/technical/cyber-exploits/2013/05/ready-for-summer-the-sunshop-campaign.html and http://www.fireeye.com/blog/technical/cyber-exploits/2013/08/the-sunshop-campaign-continues.html.

MD5 Hash	Compile Time	Malware Family
218548a9fa75febadc2562b45207efc6	1/20/13 03:25	Trojan.APT.Gh0st
2b6605b89ead179710565d1c2b614665	3/12/13 21:04	Trojan.APT.PoisonIvy
0fafed2724cb3e8a7b967c808a9fd61c	3/12/13 21:09	Trojan.APT.PoisonIvy
5fa521e8de8cbed7c176c632ae44b3d7	4/3/13 19:13	Trojan.APT.9002
d99ed31af1e0ad6fb5bf0f116063e91f	4/27/13 15:56	Trojan.APT.9002
b0ef2ab86f160aa416184c09df8388fe	4/27/13 15:56	Trojan.APT.9002
6bc1d036c6dda828b1987342d06646b2	4/27/13 15:56	Trojan.APT.9002
42bd5e7e8f74c15873ff0f4a9ce974cd	4/27/13 15:56	Trojan.APT.9002
d9eafd20eba6afedd542f2bf5b328016	4/27/13 15:56	Trojan.APT.9002
6fe0f6e68cd9cc6ed7e100e7b3626665	4/27/13 09:21	Trojan.APT.Briba
53c5570178403b6fbb423961c3831eb2	6/25/13 01:19	Trojan.APT.9002
f4ba5fd0a4f32f92aef6d5c4d971bf14	6/25/13 01:19	Trojan.APT.9002
33299011f0d2b92d951471bbc3ea52b6	8/24/13 18:22	Trojan.APT.9002
74fca616de1048c23fed5f92c4face95	8/24/13 18:22	Trojan.APT.9002
234aae60b386bd684569408c3262de03	8/24/13 18:22	Trojan.APT.9002

Table 2: Sunshop-related malware compile times

Cluster 2: DTL

The DTL campaign appears to depend primarily on spear-phishing email as an initial infection vector. We found seven different samples linked to the DTL campaign. All of these samples were detected as Trojan.APT.9002. These samples were compiled between September 19, 2012 and July 30, 2013. All of these samples were packaged with the DTL PE resource, and one of the samples was signed with the digital certificate from `Mgame Corp`.

When executed, the DTL samples called back to these CnC servers:

- `dtl.eatuo[.]com`
- `dtl.dnsd[.]me`
- `dtl6.mooo[.]com`
- `img.advertisingsee[.]com`

The campaign targeted these industries:

- Federal government
- State and local government
- Services/Consulting/VAR
- Financial services
- Telecommunications
- Aerospace/Defense/Airlines
- Energy/Utilities/Petroleum refining
- Healthcare/Pharmaceuticals
- Entertainment/Media/Hospitality
- Insurance
- Chemicals/Manufacturing/Mining
- High-tech
- Higher education

MD5 Hash	Compile Time	Malware Family
6b4aa596e5a4208371942cdb0e04dfd9	9/19/12 18:07	Trojan.APT.9002
6cbd49bed74f7bec642a4c518a99d8c5	10/10/12 15:01	Trojan.APT.9002
9f5e9e6b0c87cad988f4a486e20bbc99	3/15/13 01:55	Trojan.APT.9002
ea01e2544341da802b93fa62e6d804ed	3/15/13 01:55	Trojan.APT.9002
0b0b1f2f8f9308472c43cc41838c519f	3/15/13 01:55	Trojan.APT.9002
0e31a10218fea5b17037fde8474c809b	7/30/13 01:46	Trojan.APT.9002
a0439dcad9a30e12a5d7cb4e38d0369c	7/30/13 01:46	Trojan.APT.9002

Table 3: DTL-related malware compile times

Cluster 3: Ru.pad62

The Ru.pad62 campaign appears to utilize both spear-phishing email and strategic Web compromise as initial infection vectors. We found 26 different samples linked to the Ru.pad62 campaign. These samples were detected as Trojan.APT.9002, Trojan.APT.Gh0st, Trojan.APT.Kaba, and Trojan.APT.PoisonIvy. The 26 linked samples had compile timestamps between September 19, 2011 and December 19, 2012. Ten of the samples from the Ru.pad62 campaign were packaged with the DTL resource, and six of the samples were packaged with the Sunshop resource. Only four samples linked to the Ru.pad62 campaign were signed with digital certificates—two with the `Mgame Corp.` certificate and two with a certificate from `Microsoft`.

When executed, the Ru.pad62 samples we found called back to these CnC servers:

- ru.pad62[.]com
- tank.hja63[.]com
- 173.234.184[.]45
- fly.pad62[.]com
- tho.pad62[.]com
- tho.hja63[.]com

The campaign targeted these industries:

- Higher education
- Entertainment/Media/Hospitality
- High-tech

MD5 Hash	Compile Time	Malware Family
ea6de0e20fa5ee7c1f2cd5676c0ab7e2	9/19/11 23:11	Trojan.APT.Gh0st
ec79969351717f5197dd4b2b164d4317	9/19/11 23:11	Trojan.APT.Gh0st
e6b3febc971c711de74caea0887cf586	4/9/12 10:29	Trojan.APT.9002
bd16d4ca446f46349edbd53e06f0d01a	7/8/12 14:55	Trojan.APT.9002
625daa7c44d1d1035d455f003b6b6b5b	7/7/12 10:14	Trojan.APT.Gh0st
036863c78cc09f511fcbc29eb5bc6760	7/8/12 14:55	Trojan.APT.9002
a89a13462e1de9241569b24b101efe4d	7/8/12 14:55	Trojan.APT.9002
ef29ec86455c1abb55cf612f7a191b03	7/8/12 14:55	Trojan.APT.9002
1bd468332c0dfc8ba2a3a5f286f20b7a	7/21/12 14:50	Trojan.APT.9002
859301c5874ca3739e8ac81ddfc676e6	7/21/12 14:50	Trojan.APT.9002
58e81154a87cc93d546c4c45de9b1ec3	7/21/12 14:50	Trojan.APT.9002
6ef66c2336b2b5aaa697c2d0ab2b66e2	7/21/12 14:50	Trojan.APT.9002
d2c53f8ef8f8c04237e6c2b5e4820457	8/19/12 08:23	Trojan.APT.Kaba
50d0e9d32f8c2b3e32d073ed4a08091e	8/19/12 08:23	Trojan.APT.Kaba
841f00641de924117e2cbe6b4620015b	9/24/12 04:10	Trojan.APT.Gh0st
fce13d50bcbeae38e44b08be21f907da	9/27/12 00:13	Trojan.APT.PoisonIvy
8831d9d04aa7fdcfa1b5bdb83f71316a	9/27/12 00:13	Trojan.APT.PoisonIvy
bde732368bc01b988a6f352898259a30	12/19/12 20:25	Trojan.APT.9002
8f5c46630af8cef723995d69fe03c73f	12/19/12 20:25	Trojan.APT.9002

table continued on page 18

table continued from page 17

MD5 Hash	Compile Time	Malware Family
13c4083bdb893c8a0bd2930fa55962ca	12/19/12 20:25	Trojan.APT.9002
0bb911278eb426be95e79b7f9c5dea92	10/10/12 15:01	Trojan.APT.9002
bd2f28f776ae306eda90229b0fa13b6b	12/19/12 20:25	Trojan.APT.9002
13c4083bdb893c8a0bd2930fa55962ca	12/19/12 20:25	Trojan.APT.9002
f5ffbd8d17ab21095c56e00831c79cbc	12/19/12 20:25	Trojan.APT.9002
a7481bd182886c7aae99abfd6f25d005	12/19/12 20:25	Trojan.APT.9002
aa31a6a94d4ad7bf494b2532f2f7cb63	10/10/12 15:01	Trojan.APT.9002
4eff545f1e04946e0b088ed15873b02d	10/10/12 15:01	Trojan.APT.9002

Table 4: Ru.pad62-related malware and compile times

Cluster 4: Downmicrisoft

The Downmicrisoft campaign appears to utilize strategic Web compromise as an initial infection vector. We found five different samples linked to the Downmicrisoft campaign. These samples were detected as Trojan.APT.9002 and Trojan.APT.Gh0st. The five samples had compile timestamps between December 19, 2012 and April 4, 2013. The earliest compile time for samples from the Downmicrisoft campaign (December 19, 2012) was the same day as the latest compile time for samples from the Ru.Pad62 campaign. Three of the samples linked to the Downmicrisoft campaign were packaged with the Sunshop PE resource, and all but one sample was signed with the `Mgame Corp.` digital certificate.

When executed, the Downmicrisoft samples called back to these CnC servers:

- `wv.downmicrisoft[.]com`
- `mx.downmicrisoft[.]com`
- `up.downmicrisoft[.]com`
- `tebit-newtwn.ftpmicrosoft[.]com`
- `twn.ftpmicrosoft[.]com`

The campaign targeted these industries:

- Entertainment/Media/Hospitality
- High-tech

The same media organization targeted in the Downmicrisoft campaign was also targeted in the Ru.Pad62 campaign.

MD5 Hash	Compile Time	Malware Family
c8589ec3171656514ebd4df4cb79ec89	12/19/12 20:25	Trojan.APT.9002
82fc8465c01c416c6dcaeaf16822d5a3	12/19/12 20:25	Trojan.APT.9002
71e761d1683e76d5741cdf2d05aecdf8	12/19/12 20:25	Trojan.APT.9002
372d218077715661aea2ada27b16e500	12/19/12 20:25	Trojan.APT.9002
c27730971c04cdf049b44912a50b4804	4/4/13 09:50	Trojan.APT.Gh0st

Table 5: Downmicrisoft-related malware and compile times

Also, the Trojan.APT.Gh0st sample linked to the Downmicrisoft campaign, `c27730971c04cdf049b44912a50b4804`, did not use the default "`Gh0st`" string. Instead, this sample used the string "`HTTPS`". Gh0st variants with this same string were described by RSA in a 2012 paper.[7]

Cluster 5: Boeing-Job

The Boeing-Job campaign appears to utilize strategic Web compromises as an initial infection vector. We previously discussed the Boeing-Job campaign's use of the "Lady Boyle" Flash exploit on the FireEye blog.[8] We identified 19 different samples linked to the Boeing-Job campaign. These samples were all detected as Trojan.APT.9002 and had compile timestamps between July 21, 2012 and April 3, 2013. Seven of the samples from the Boeing-Job campaign were packaged with both the Sunshop PE resource, and all but two were signed with the `Mgame Corp.` digital certificate.

When executed, the Boeing-Job samples called back to these CnC servers:

- `www.boeing-job[.]com`
- `engage.intelfox[.]com`
- `ieee.boeing-job[.]com`
- `lol.dns-lookup[.]us`
- `127.0.0.1`

The campaign targeted these industries:

- Financial services
- Energy/Utilities/Petroleum refining
- Telecommunications

7 RSA. "The Voho Campaign: an In Depth Analysis." September 2012.

8 Thoufique Haq and J. Gomez. "LadyBoyle Comes to Town with a New Exploit." February 2013.

MD5 Hash	Compile Time	Malware Family
a24992c89c4a8dd83b5e910131054c60	7/21/12 14:50	Trojan.APT.9002
a7c79c7e13a6f3e5bfe4852efd937096	12/19/12 20:25	Trojan.APT.9002
2a7e98b3079af88e296ed934966486b7	12/19/12 20:25	Trojan.APT.9002
d399e5b8d0d6a01e14e713488d1ee6d9	12/19/12 20:25	Trojan.APT.9002
fb53093f42b7517822f15cfd20cc24fe	12/19/12 20:25	Trojan.APT.9002
94b564a3881bf4c3fcd1cc1c5f44e72f	12/19/12 20:25	Trojan.APT.9002
7826651ee38c7e8d46131806b0bca1c6	12/19/12 20:25	Trojan.APT.9002
f1ba92689036ab3c3aec7e0d49a647f1	12/19/12 20:25	Trojan.APT.9002
47eec3b99a8dfa5381f24d6518bb7eda	12/19/12 20:25	Trojan.APT.9002
fce973f7983b06b85aba0cab17732178	12/19/12 20:25	Trojan.APT.9002
744a6a6c6b0f7b7355b7c1d5f1efd46e	12/19/12 20:25	Trojan.APT.9002
bd4dc30072f76f20b52e0c564473bc92	12/19/12 20:25	Trojan.APT.9002
97cd618e80cdc79353290cffb17274b8	12/19/12 20:25	Trojan.APT.9002
432dce23d00694b103dd838144253d1b	12/19/12 20:25	Trojan.APT.9002
a022f14ba32aeff2fe416a11384ed0ef	1/22/13 23:38	Trojan.APT.9002
b4da1c3400b48803b41823feaf6085e8	2/4/13 16:15	Trojan.APT.9002
b8ef95a8b32d31f29db5ca6b530815b9	2/4/13 16:15	Trojan.APT.9002
432dce23d00694b103dd838144253d1b	2/4/13 16:15	Trojan.APT.9002
ebd2bc0beecb9d3f80bbfaf7e046b31f	2/4/13 16:15	Trojan.APT.9002

Table 6: Boeing-Job-related malware and compile times

Cluster 6: Google-blogspot

The Google-blogspot campaign appears to utilize strategic Web compromise as an initial infection vector. We identified seven different samples linked to the Google-blogspot campaign. These samples were all detected as Trojan.APT.Gh0st or Trojan.APT.PoisonIvy. The Google-blogspot samples had compile timestamps between September 16, 2008 and June 27, 2012. Four of the samples from the Google-blogspot campaign were packaged with the Sunshop PE resource, and one sample was signed with a digital certificate from `Facesun.cn`.

When executed, the Google-blogspot samples called back to these CnC servers:

- `soft.google-blogspot[.]com`
- `www.google-blogspot[.]com`
- `blog.googleblog.iego[.]net`

The campaign targeted this industry:

- Healthcare/Pharmaceuticals

MD5 Hash	Compile Time	Malware Family
2eee37b222ba9e8f373e49d31af62a69	9/16/08 10:17	Trojan.APT.Gh0st
e21c3c26c801573b789b39a0ff3c549b	12/20/11 00:32	Trojan.APT.Gh0st
ab468267b60a087ea8ad2a35a00e4f08	6/27/12 15:51	Trojan.APT.Gh0st
9ffe2463e87a424b8cd7c8d1c77dc2bb	6/27/12 15:51	Trojan.APT.Gh0st
1a24e834b4c7dd16f988ab590d03194d	6/27/12 15:51	Trojan.APT.Gh0st
959a6f30de52b481c31e4482fea4333c	6/27/12 15:51	Trojan.APT.Gh0st
bb610bc9fbff3dd473b10a07ae963499	2/22/13 09:11	Trojan.APT.PoisonIvy

Table 7: Google-blogspot related malware and compile times

Cluster 7: Luckme

The Luckme campaign appears to utilize strategic Web compromise as an initial infection vector. We identified 18 different samples linked to the Luckme campaign. These samples were all detected as Trojan.APT.PoisonIvy and had compile timestamps between April 3, 2011 and April 3, 2013. Four of the samples from the Luckme campaign were packaged with the Sunshop PE resource. Fifteen of the Luckme samples were signed with the digital certificate from `Wuhan Tian Chen Information Technology Co., Ltd`.

When executed, Luckme samples called back to these CnC servers:

- `luckmegame.servegame[.]com`
- `luckmevnc.myvnc[.]com`
- `huangma.dyndns[.]org`
- `zhouweb.dyndns[.]info`
- `frontpage.dyndns[.]org`
- `frontpage.dhis[.]org`
- `blankorder.zapto[.]org`
- `blankorder.dyndns-mail[.]com`
- `registrat.dyndns[.]org`
- `registrat.zapto[.]org`

The campaign targeted these industries:

- High-tech
- Aerospace/Defense/Airlines
- Federal government
- Services/Consulting/VAR

MD5 Hash	Compile Time	Malware Family
01a3edddd7c130048b24822277c507f0	4/3/11 01:29	Trojan.APT.PoisonIvy
b885c7d2616ca27cb408efcd8328dd36	4/20/11 02:53	Trojan.APT.PoisonIvy
7d41640e7dbf7b4a3c6dc147b994b01b	7/2/11 08:54	Trojan.APT.PoisonIvy
9f729cb50867edcb71116df67a32ff24	6/9/12 03:10	Trojan.APT.PoisonIvy
184a9d13616702154fb10ff9c5d67041	6/9/12 03:10	Trojan.APT.PoisonIvy
89c54a39b64361df19ce5a2de14c47c6	9/18/12 16:22	Trojan.APT.PoisonIvy
2b1675ac31a158e2518b3fbe77e935f1	10/19/12 14:39	Trojan.APT.PoisonIvy
bf75391e4aa5e812d138c53e24e17d9e	10/19/12 14:39	Trojan.APT.PoisonIvy
96ad6bd5416571118a9e9b8d1cb9b8ee	10/19/12 14:39	Trojan.APT.PoisonIvy
f7ea36b555afe376427f6c32ade78595	10/19/12 16:59	Trojan.APT.PoisonIvy
20728edd9a17e0a85719553115b25ec2	10/19/12 16:59	Trojan.APT.PoisonIvy
21c9da542789db45db0c0e5389a49c46	10/19/12 16:59	Trojan.APT.PoisonIvy
3caf55608384a6dfd98fb9c076863b7b	10/19/12 16:59	Trojan.APT.PoisonIvy
2b825e46ae60a9d15b5a731e57410425	10/19/12 17:45	Trojan.APT.PoisonIvy
011bc59a3dd478475bcd033cf09fa93a	10/19/12 17:45	Trojan.APT.PoisonIvy
ca22207c5441a100437b75d7ce0d3fe2	3/5/13 02:19	Trojan.APT.PoisonIvy
b08f2ae0542f60f463fcd160ec1e9355	4/3/13 23:00	Trojan.APT.PoisonIvy
09d4c2f1f24fbdcb1c286b2f4c5589d2	4/3/13 23:00	Trojan.APT.PoisonIvy

Table 8: Luckme-related malware and compile times

Cluster 8: Piping

The Piping campaign appears to utilize strategic Web compromise as an initial infection vector. We identified four different samples linked to the Piping campaign. These samples were detected as Trojan.APT.PoisonIvy and Trojan.APT.9002. The Piping linked samples had compile timestamps between December 19, 2012 and January 2, 2013. All of the samples from this campaign were packaged with the Sunshop PE resource, and none was signed with a digital certificate.

When executed, the Piping samples called back to these CnC servers:

- koko4w.no-ip[.]org
- okok4o.zapto[.]org
- blabla4m.no-ip[.]org
- piping.no-ip[.]org

The campaign targeted these industries:

- Chemicals/Manufacturing/Mining
- Financial services
- Energy/Utilities/Petroleum refining
- Healthcare/Pharmaceuticals
- High-tech

MD5 Hash	Compile Time	Malware Family
ef4070380ed10008111102f575139b3d	12/19/12 20:25	Trojan.APT.9002
76e7f9bd532e4204b749cb739d6ada1b	1/2/13 16:23	Trojan.APT.PoisonIvy
afc4d73bde2a536d7a9b7596288ce180	1/2/13 16:26	Trojan.APT.PoisonIvy
25f38271e2a3d55a83917f1b9825fde9	1/2/13 16:27	Trojan.APT.PoisonIvy

Table 9: Piping-related malware and compile times

Cluster 9: Update1

The Update1 campaign appears to utilize strategic Web compromise as an initial infection vector. We identified five different samples linked to the Update1 campaign. All of these samples were detected as Trojan.APT.9002 and had compile timestamps between July 30, 2012 and December 19, 2012. One of the Update1 samples was packaged with the Sunshop PE resource and one was packaged with the DTL PE resource. None of the samples was signed with a digital certificate.

When executed, the Update1 samples called back to these CnC servers:

- `update1.mysq1[.]net`
- `update.mysq1[.]net`
- `pack.fartit[.]com`
- `updatedns.itemdb[.]com`

The campaign targeted these industries:

- High-tech
- Entertainment/Media/Hospitality
- Applied research and development
- Services/Consulting/VAR

MD5 Hash	Compile Time	Malware Family
9322365a4b89556b033b0ab90e43a68a	7/30/12 05:37	Trojan.APT.9002
b0b8db07a5126e6a8e15299efe74d068	8/23/12 20:49	Trojan.APT.9002
bdc562e2752fa7da15772906358bb082	8/24/12 14:36	Trojan.APT.9002
0f8c4da83642efa4a70d9c8e52b67ba5	8/24/12 14:36	Trojan.APT.9002
4cd171813a2d9d2152f7a7428d5348eb	12/19/12 20:25	Trojan.APT.9002

Table 10: Update1-related malware and compile times

Cluster 10: Packets

The Packets campaign appears to utilize spear-phishing email as an initial infection vector. We identified one Trojan.APT.9002 sample linked to the Packets campaign. This sample had a compile time of December 19, 2012 and was packaged with the Sunshop PE resource. The sample was not signed with a digital certificate. It called back to this CnC server:

- mlog.ddns[.]us

MD5 Hash	Compile Time	Malware Family
bfaf33f80815471646dc007f7ac18f7b	12/19/12 20:25	Trojan.APT.9002

Table 11: Packets-related malware and compile times

Cluster 11: Allshell

The Allshell campaign appears to utilize spear-phishing email as a vector to attack its targets. We identified one Trojan.APT.9002 sample linked to the Allshell campaign. This sample had a compile time of October 16, 2012 and was packaged with the DTL PE resource. The sample was not signed with a digital certificate. It called back to this CnC server:

- stmp.allshell[.]net

The campaign targeted these industries:

- High-tech
- Aerospace/Defense/Airlines

MD5 Hash	Compile Time	Malware Family
0c6b69976fa75b477fcece125b4b0e96	10/16/12 19:45	Trojan.APT.9002

Table 12: Allshell-related malware and compile times

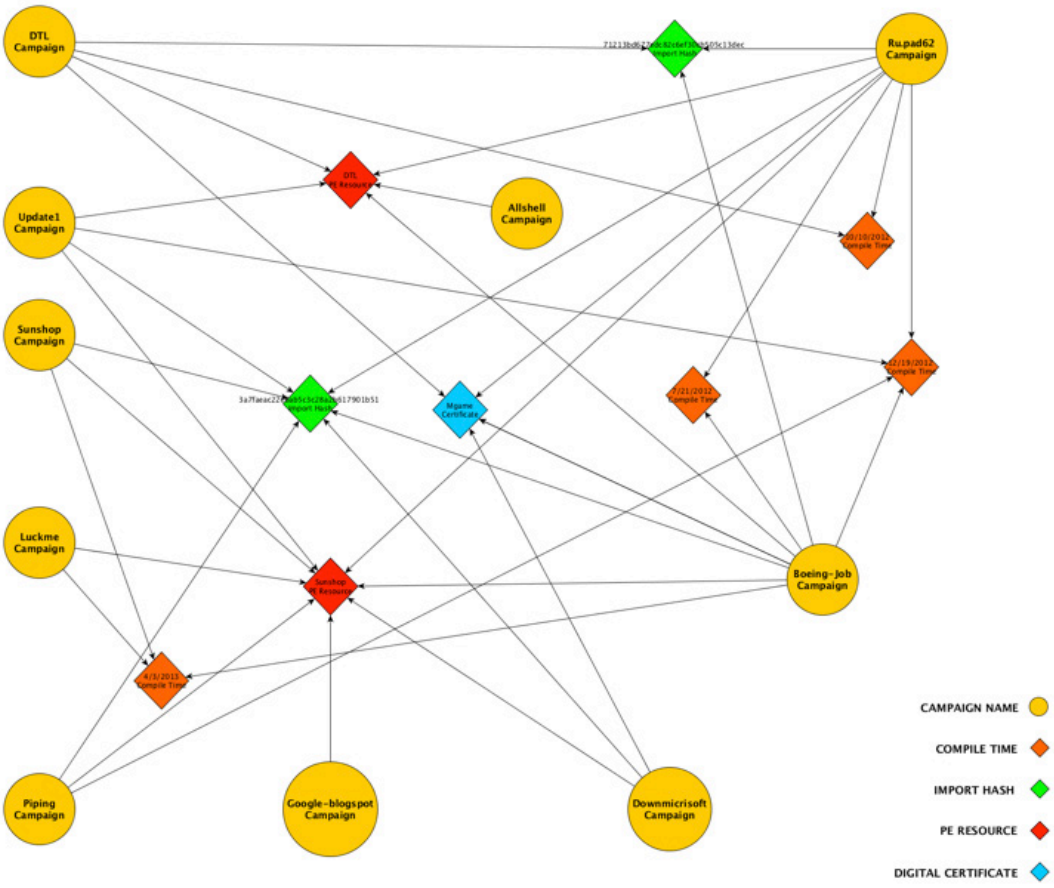

Figure 8: A graphic illustration of the relationships seen across the 11 different campaigns

Shared Builders

These observed shared characteristics across these malware samples are likely the result of a set of common "builders" developed by a shared development and logistics infrastructure.

Builders are tools used by malicious actors to quickly and easily create different variants of the same malware. In a typical scenario, a skilled developer creates a builder and shares it with an operator more skilled in intrusion operations than in code development. This separation of tasks is more efficient and supports a faster tempo of offensive operations. A typical builder provides a graphical user interface that enables a threat actor to configure elements such as the location of the CnC server.

To recap, these shared characteristics, as discussed in previous sections, include the following:

- The Sunshop and DTL PE resources
- Common import tables
- Six different digital certificates
- Common compile times
- Common malware families

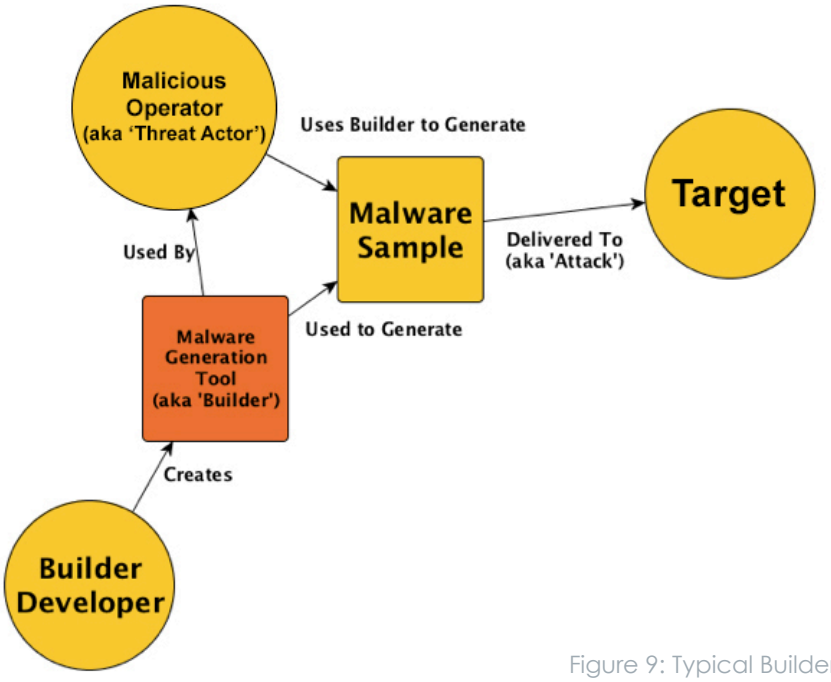

Figure 9: Typical Builder life cycle

We identified a builder tool used to create Trojan.APT.9002 binaries, which we are dubbing "9002 Builder." This builder generates Trojan.APT.9002 binaries with the DTL resource.

Figure 10: Builder used to generate Trojan.APT.9002 malware

As shown in Figure 10, the dialogue and menu options in this GUI are in Chinese. The builder enables threat actors to configure the following:

- Both a primary and a secondary CnC server.
- A specific ID. The default ID produced by this builder is "1."
- An "Internet health check" domain. The default health check domain configured in this builder was "update.microsoft.com". An Internet health check domain is typically used by malware to determine whether a target's endpoint is connected to the Internet before acting.
- Proxy settings, including address/port, type, proxy authentication details, auto-detect proxy, and force-proxy only.

Also, the text in the title bar of this builder is "[User_Server_Builder] update 2012-7-21". Although the servers produced by this builder have a compile time of 10/23/12 8:30 UTC, we believe the date in the title bar of the builder is significant; we identified five different binaries with a compile time of 7/21/12. All five utilized the same DTL resource found in 9002 Builder.

MD5 Hash	Compile Time	CnC Server	PE Resource
a24992c89c4a8dd83b5e910131054c60	7/21/12 14:50	engage.intelfox[.]com	DTL
1bd468332c0dfc8ba2a3a5f286f20b7a	7/21/12 14:50	ru.pad62[.]com	DTL
859301c5874ca3739e8ac81ddfc676e6	7/21/12 14:50	ru.pad62[.]com	DTL
58e81154a87cc93d546c4c45de9b1ec3	7/21/12 14:50	ru.pad62[.]com	DTL
6ef66c2336b2b5aaa697c2d0ab2b66e2	7/21/12 14:50	tank.hja63[.]com	DTL

Table 13: Malware samples created by a builder using the same DTL resource found in 9002 Builder

The 9002 Builder appears to be a modified variant of the builder used to create the samples listed in Table 12. The compile time of the builder is 10/23/2012 11:18 UTC, a little less than 3 hours after the compile time of the server that is produced by it. We believe it is a common practice for the developer to compile a new server, update the builder code accordingly, then compile the new builder. The older date in the title bar may just be an oversight as it would have to be manually updated by the developer.

The builder contains a copy of the server executable in its PE resource section, under `BIN`. The server executable is responsible for installing the 9002 payload malware, and has its configuration block stored in its `.data` section, with some default settings including the CnC pointing to `192.168.8.105`. The configuration block uses simple, single-byte XOR encryption. The key varies from version to version; in some cases, it skips null bytes. During the installation routine, the configuration block is written to the registry value `sysinfo` under the registry key `HKCU\Software\Classes`.

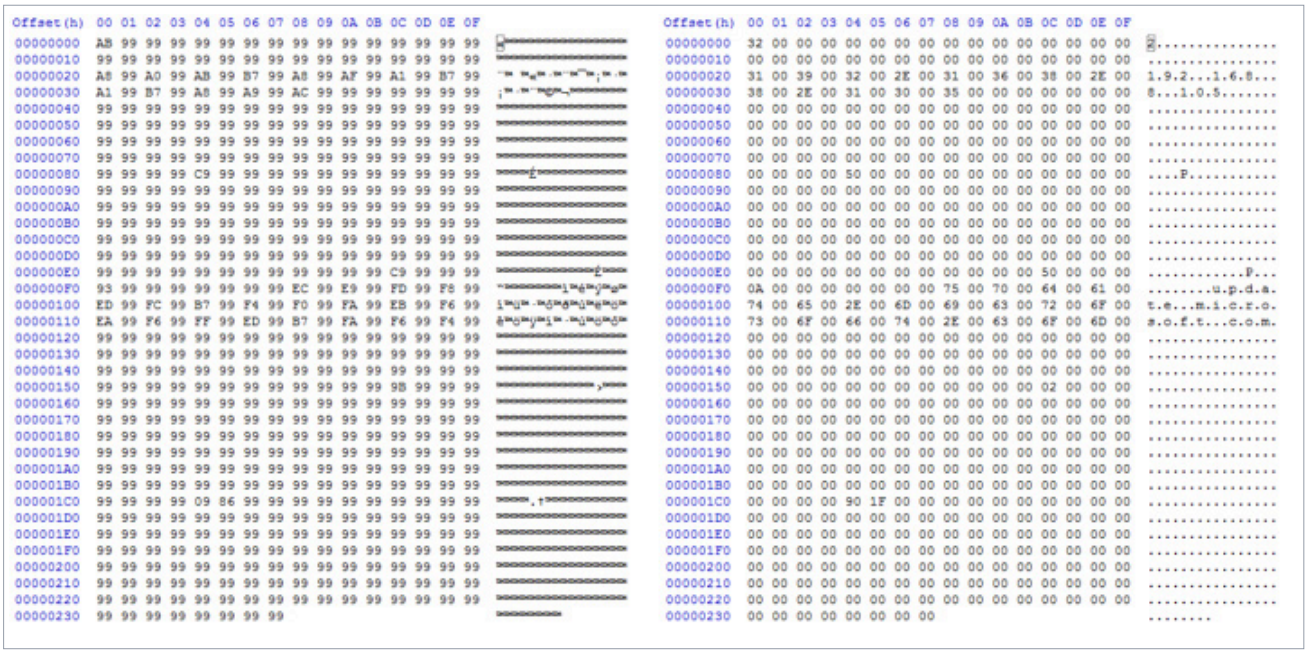

Figure 11: 9002 Builder configuration block before (left) and after (right) XOR decryption

When the threat actor builds a malware executable, the builder writes the server executable to disk and overwrites the configuration block with the newly configured options. The location of the configuration block within the `.data` section is hard-coded, meaning that the builder must be modified each time the server code is updated and the location of the configuration block changes. We noticed that the configuration block is indeed stored at a different offset in the samples compiled on 7/21/12 as compared to the sample created by the builder we have with the compile date of 10/23/12. This further supports our belief in the practice of the developer compiling the server and then shortly after compiling the builder. He would need time to locate the new offset of the configuration block in the newly compiled server executable and then change the hard-coded value in the builder code.

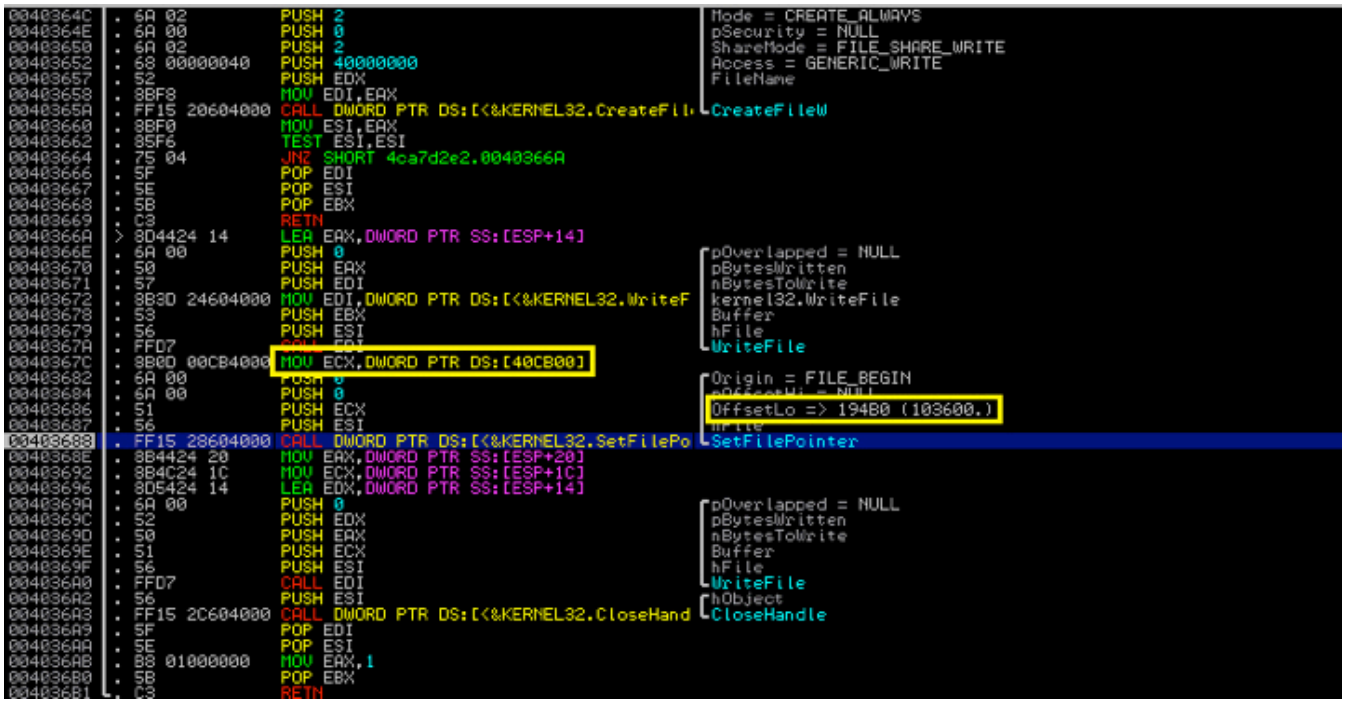

Figure 12: 9002 Builder code, with hard-coded offset to the server's configuration block

Attackers using 9002 Builder seem to have gradually adopted another launcher that stores the configuration block as a resource instead of storing it in its `.data` section. Based on the compile-time analysis outlined in the "Compile Times" section of this report, the shift began in late October of 2012 (with a few exceptions). This shift makes sense for the builder's developer(s); they no longer needed to update the builder for every code change in the launcher or 9002 payload malware. This launcher, mentioned earlier in this paper as having the import table hash `3a7faeac22e6ab5c3c28a2b617901b51`, supports different payloads, such as Poison Ivy and 9002.

Conclusion

Based on the evidence provided, we draw the following possible conclusions:

[High Confidence] SDQ exists and supports separate APT campaigns. We believe the most likely explanation for these documented correlations is that a shared 'development and logistics' operation (SDQ) supports a number of different APT campaigns, as part of formal offensive apparatus.

[Low Confidence] SDQ and APT campaigns are a single actor. That said, it is conceivable that the 11 clusters of activity, previously believed to be independent campaigns run by different actors, are in fact one cluster of activity run by one well-resourced actor. However, we believe this scenario is less likely because each cluster of activity utilized malware samples with different artifacts such as passwords, campaign identifiers, and mutexes. These artifacts were generally consistent within each cluster of activity but differed across clusters.

[Medium Confidence] SDQ does not exist, and APT actors informally share among each other. Alternatively, different actors might be responsible for the documented 11 clusters of activity and instead of relying on a centralized development and logistics operation, these actors share TTPs through formal or informal channels.

In each of these scenarios, a shared development and logistics infrastructure or some notion of a digital quartermaster clearly underpins all of the activity presented in this report. Whether this quartermaster involves informal connections between developers or a structured bureaucratic organization serving a central offensive apparatus is unclear. Regardless of the scenario, the overall finding of a shared development and logistics infrastructure suggests targeted organizations are facing a more organized menace than they realize.

Appendix A: Authenticode/Digital Certificates

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            4e:eb:08:05:55:f1:ab:f7:09:bb:a9:ca:e3:2f:13:cd
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=ZA, O=Thawte Consulting (Pty) Ltd., CN=Thawte Code Signing CA
        Validity
            Not Before: Jun 19 00:00:00 2009 GMT
            Not After : Jun 19 23:59:59 2011 GMT
        Subject: C=KR, ST=Seoul, L=Geumcheon-gu, O=MGAME Corp., OU=Web Dev Team,
CN=MGAME Corp.
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:c5:6a:00:76:7b:80:ce:08:78:aa:75:47:46:2a:
                    1b:42:e4:b8:bc:a3:10:1a:6d:29:31:fd:dd:21:1e:
                    27:9a:3a:39:c8:66:0d:7d:bd:da:74:cc:09:b7:51:
                    60:36:80:2e:da:f4:bd:b7:9c:8b:a2:f5:35:aa:d2:
                    4f:a5:0a:a4:77:5e:3b:fd:45:86:96:f0:00:d3:3b:
                    97:87:49:99:1e:8f:f3:0d:d9:cc:55:86:12:c0:5f:
                    9e:ed:d2:6e:34:12:f1:69:33:ff:09:ef:49:fc:95:
                    d8:19:01:d9:bc:99:27:92:0b:b5:98:91:a1:2f:24:
                    e1:dc:17:ae:2b:e1:85:c6:19
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 CRL Distribution Points:
                URI:http://crl.thawte.com/ThawteCodeSigningCA.crl

            X509v3 Extended Key Usage:
                Code Signing, Microsoft Commercial Code Signing
            2.5.29.4:
                0.0.0..
+.....7.......
            Authority Information Access:
                OCSP - URI:http://ocsp.thawte.com
```

```
            Netscape Cert Type:
                Object Signing
    Signature Algorithm: sha1WithRSAEncryption
        8c:ea:48:e7:9f:4e:d9:49:9c:54:b2:56:02:0a:ce:d5:3a:5b:
        b7:2b:a6:8b:c2:13:08:6d:13:8f:17:af:d8:96:5c:13:f5:80:
        5a:ec:bd:e7:be:76:85:84:76:82:6a:23:af:47:1b:0c:c4:fe:
        a3:cc:59:21:fd:c6:97:32:8b:6c:f3:34:ed:b3:b1:2a:4a:b3:
        22:60:83:06:3b:36:c9:6c:c0:78:08:5c:de:1c:3d:09:49:73:
        a7:35:22:27:d6:19:ee:41:f6:10:fc:64:78:dc:dc:b2:79:82:
        2a:61:2f:3e:cb:d7:7f:cf:fe:0f:4e:ab:47:d6:94:5b:84:40:
         f7:20
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            da:61:49:95:64:a7:f1:8e:be:8b:03:b7:12:c2:9e:09
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=US, O=WoSign, Inc., CN=WoSign Code Signing Authority
        Validity
            Not Before: Aug 13 00:00:00 2010 GMT
            Not After : Aug 13 23:59:59 2011 GMT
        Subject: C=CN, ST=\xE6\xB9\x96\xE5\x8C\x97\xE7\x9C\x81, L=\xE6\xAD\xA6\xE6\
xB1\x89\xE5\xB8\x82, O=\xE6\xAD\xA6\xE6\xB1\x89\xE5\xA4\xA9\xE5\xAE\xB8\xE4\xBF\xA1\
xE6\x81\xAF\xE6\x8A\x80\xE6\x9C\xAF\xE6\x9C\x89\xE9\x99\x90\xE5\x85\xAC\xE5\x8F\xB8,
OU=WoSign Class 3 Code Signing, CN=\xE6\xAD\xA6\xE6\xB1\x89\xE5\xA4\xA9\xE5\xAE\xB8\
xE4\xBF\xA1\xE6\x81\xAF\xE6\x8A\x80\xE6\x9C\xAF\xE6\x9C\x89\xE9\x99\x90\xE5\x85\xAC\
xE5\x8F\xB8
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:ad:12:17:ee:5a:5a:a7:9f:ee:60:08:58:30:8d:
                    5d:2d:90:c6:ed:fd:20:53:7b:fe:23:44:77:4b:a9:
                    25:ca:b0:5d:d6:c8:3a:e5:1f:a5:bb:7e:f4:65:75:
                    c7:2c:34:4e:4f:ea:a0:43:1f:10:ee:97:e8:7c:0e:
                    83:f6:09:ab:90:d0:5e:0b:36:2e:eb:7a:39:2c:fa:
                    7f:1a:b8:9d:5d:2e:3b:24:71:4a:3b:0a:a9:46:e1:
                    8e:28:a6:85:9c:da:52:f1:b0:6e:57:6f:24:81:bf:
                    cf:36:1b:5a:95:d7:35:cb:c9:61:56:ac:3c:e4:cd:
                    73:66:a2:42:2a:32:ea:52:cc:c7:ab:9b:63:4e:a2:
                    77:d7:aa:6b:7f:14:25:15:e6:b6:f0:54:68:41:d2:
                    54:74:41:0b:6e:b8:fa:ac:22:26:94:2a:b7:2e:ce:
                    18:5e:9b:1d:0a:d1:bd:f1:b8:5a:39:b4:3e:21:1b:
```

```
                eb:ce:9b:3d:34:0f:19:fd:b3:b8:2e:13:53:80:2d:
                29:af:14:bf:33:62:d8:68:b4:3f:02:98:26:bb:d5:
                b7:69:cf:9c:f5:8a:bc:45:fd:7f:51:fa:5f:b9:33:
                fe:62:2c:cc:fc:43:34:7e:e8:9a:c0:2c:17:8c:25:
                c8:48:45:08:9f:4f:04:ce:54:c6:51:cc:3e:54:a0:
                6a:cd
            Exponent: 65537 (0x10001)
    X509v3 extensions:
        X509v3 Authority Key Identifier:
            keyid:A4:13:6A:3F:10:0B:D7:21:87:D4:8B:05:CA:BC:B1:02:CD:54:E2:8A

        X509v3 Subject Key Identifier:
            CB:DD:A1:49:1B:B3:17:85:BB:B1:A0:2D:33:18:82:39:9A:7B:CA:6F
        X509v3 Key Usage: critical
            Digital Signature
        X509v3 Basic Constraints: critical
            CA:FALSE
        X509v3 Extended Key Usage:
            Code Signing, Microsoft Commercial Code Signing
        X509v3 Certificate Policies:
            Policy: 1.3.6.1.4.1.6449.1.2.2.22
              CPS: http://www.wosign.com/cps/

        X509v3 CRL Distribution Points:
            URI:http://crl.wosign.com/WoSignCodeSigning.crl

        Authority Information Access:
            CA Issuers - URI:http://crt.wosign.com/WoSignCodeSigning.crt

Signature Algorithm: sha1WithRSAEncryption
    8d:89:24:cc:ea:3f:23:af:01:46:59:24:43:22:67:b3:27:74:
    84:fc:ae:ea:03:bc:09:b5:f0:88:8a:13:01:d3:4f:d7:a9:01:
    c3:4c:5e:46:02:b5:46:e3:25:02:fc:f9:e3:f6:41:79:fa:18:
    c5:0f:96:06:78:db:ed:51:35:55:4b:d2:b3:07:11:13:f2:a9:
    75:99:5e:ac:67:6a:3c:9f:a6:73:8a:4b:f4:ac:8c:a2:6b:e4:
    d6:a2:00:46:a5:73:11:d7:ca:e5:99:cd:68:b0:e3:ff:76:36:
    f4:62:a5:71:73:0c:cc:a5:79:e4:54:a2:7b:25:de:72:6b:0d:
    67:ba:43:ec:98:26:da:bc:6a:bd:7e:29:c9:d2:75:b7:ac:6d:
    c9:d1:3b:e0:ef:9d:e9:1e:4a:17:fd:bd:81:6e:96:1e:13:f9:
    7a:bf:66:ae:6b:7d:55:be:ce:71:0c:b7:e8:fd:da:72:58:fb:
    0c:8b:d0:ec:6e:35:f3:be:02:cb:c1:40:8b:94:1d:24:32:8a:
```

```
        d7:84:fd:94:66:a2:65:7c:ca:f9:c1:27:b7:53:42:14:47:1a:
        97:91:6f:87:e5:a5:02:63:69:79:9b:e2:a6:1c:67:eb:f4:ac:
        42:91:47:79:51:fe:20:df:4a:49:b4:b2:a1:78:1f:22:60:0d:
        0f:ca:b4:6e
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            37:3e:80:24:1c:d2:98:b0:4e:85:24:62:41:42:13:fc
        Signature Algorithm: md5WithRSAEncryption
        Issuer: CN=Root Agency
        Validity
            Not Before: Feb 21 06:00:46 2013 GMT
            Not After : Dec 31 23:59:59 2039 GMT
        Subject: O=T\x09ye[\x891\xF0/emailAddress=John-hotmail-com, CN=Facesun.cn
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:c4:dc:fb:70:09:61:88:95:a5:1a:dd:c9:5c:dd:
                    c5:5b:3c:42:1a:f4:34:38:fc:ae:25:45:d6:ce:c3:
                    a1:bd:60:e6:2d:34:1d:be:b3:12:66:ac:51:76:ce:
                    3f:fc:04:18:21:65:ef:f4:6f:8d:ea:a2:2e:bb:d4:
                    9e:05:ba:48:02:e7:05:2e:46:d2:26:db:ca:68:c8:
                    ec:be:cf:0a:6f:21:e0:bf:dd:bf:c9:a3:cc:4c:1d:
                    5a:47:a9:e9:8f:36:43:ab:b6:95:40:04:5f:9f:5c:
                    12:f2:18:88:b5:ae:1c:52:2b:3f:2c:0b:fd:29:d2:
                    c6:de:1b:e3:89:8c:b1:2d:29
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            2.5.29.1:
                0>.....-...O..a!..dc..0.1.0...U....Root Agency...7l...d......\5.
    Signature Algorithm: md5WithRSAEncryption
        34:1b:5f:c7:3c:a1:69:f3:3b:f3:9f:8d:09:1b:10:6a:8f:02:
        00:28:7d:45:33:a0:2e:1b:70:d4:a4:5a:a3:85:a7:c6:35:4c:
        31:6e:10:4b:91:48:4a:3d:1a:2c:cc:86:c4:e0:bd:2a:44:d7:
        94:9b:9e:e6:71:1e:b8:58:32:15

Certificate:
    Data:
        Version: 3 (0x2)
```

```
        Serial Number:
            7e:45:f7:bc:62:39:59:91:4f:5b:84:fa:b0:97:ba:b8
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=Terms of use
at https://www.verisign.com/rpa (c)04, CN=VeriSign Class 3 Code Signing 2004 CA
        Validity
            Not Before: Apr 16 00:00:00 2009 GMT
            Not After : Apr 18 23:59:59 2012 GMT
        Subject: C=CN, ST=Beijing, L=Beijing, O=SINA.COM TECHNOLOGY (CHINA) CO. LTD,
OU=Digital ID Class 3 - Microsoft Software Validation v2, CN=SINA.COM TECHNOLOGY
(CHINA) CO. LTD
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:ca:3f:cd:e7:f4:9d:19:fe:83:92:15:2c:06:8e:
                    4c:ff:7a:8d:17:0c:94:e8:3c:25:c1:c2:ed:d5:22:
                    87:b7:3c:81:c5:96:f1:94:cd:ef:19:c8:ce:13:85:
                    27:c4:75:af:f1:54:71:d5:2d:4b:7b:de:3c:ac:10:
                    e0:68:16:d5:7c:55:3f:02:ff:84:5e:31:c9:47:69:
                    3e:d9:e1:dc:50:b2:ef:04:8d:da:02:25:cb:57:96:
                    6b:e9:fe:b3:d8:db:0f:6c:c7:e8:80:db:92:ac:5b:
                    6f:76:99:dd:13:70:92:d8:93:f2:53:16:5b:00:b1:
                    a7:99:d2:3c:38:4f:4e:d9:43
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Key Usage: critical
                Digital Signature
            X509v3 CRL Distribution Points:
                URI:http://CSC3-2004-crl.verisign.com/CSC3-2004.crl

            X509v3 Certificate Policies:
                Policy: 2.16.840.1.113733.1.7.23.3
                  CPS: https://www.verisign.com/rpa

            X509v3 Extended Key Usage:
                Code Signing
            Authority Information Access:
                OCSP - URI:http://ocsp.verisign.com
                CA Issuers - URI:http://CSC3-2004-aia.verisign.com/CSC3-2004-aia.cer
```

```
            X509v3 Authority Key Identifier:
                keyid:08:F5:51:E8:FB:FE:3D:3D:64:36:7C:68:CF:5B:78:A8:DF:B9:C5:37

            Netscape Cert Type:
                Object Signing
            1.3.6.1.4.1.311.2.1.27:
                0.......
    Signature Algorithm: sha1WithRSAEncryption
        bc:99:88:52:b3:26:a3:af:b4:09:83:4e:c2:4b:91:86:6c:e4:
        50:9a:eb:27:cb:6a:e9:77:4f:b8:c3:42:0b:1d:1a:3b:21:ed:
        09:32:67:62:1a:89:86:01:55:0b:44:01:75:d9:17:59:98:0c:
        5a:2d:09:33:f5:cd:e7:ba:f4:a3:04:0a:05:40:38:6a:7f:c5:
        bb:82:aa:0b:ae:3a:b0:78:27:6b:3a:f7:d9:ba:c7:1a:13:e3:
        1d:ee:c9:b8:c7:54:c5:46:e4:8a:97:c6:07:11:45:0a:57:85:
        7c:ab:35:7b:5d:45:0b:3f:84:c6:32:43:7a:06:aa:48:52:d0:
        16:23:74:d0:e1:6d:2c:42:d1:bb:cf:f5:70:ca:27:8e:69:35:
        cc:72:b1:2d:dd:b1:9a:d1:f7:65:37:45:2e:36:c9:fd:9c:67:
        87:b6:50:f8:e9:3f:86:a0:c6:3e:3f:66:6e:0e:de:fb:dc:67:
        d6:29:f0:25:5b:2d:53:92:cf:07:70:50:38:3c:04:34:57:19:
        59:23:09:eb:44:fe:5b:40:a3:ae:ed:5f:1a:84:80:00:ab:b8:
        2a:1f:da:ef:02:46:23:b4:1e:d1:6a:90:86:9c:12:af:13:b1:
        59:63:b9:47:09:d8:ad:8a:c8:66:38:3c:44:a0:37:b4:27:9c:
        f5:ed:61:62

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            61:46:9e:cb:00:04:00:00:00:65
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=US, ST=Washington, L=Redmond, O=Microsoft Corporation,
OU=Copyright (c) 2000 Microsoft Corp., CN=Microsoft Code Signing PCA
        Validity
            Not Before: Apr  4 19:43:46 2006 GMT
            Not After : Oct  4 19:53:46 2007 GMT
        Subject: C=US, ST=Washington, L=Redmond, O=Microsoft Corporation,
CN=Microsoft Corporation
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:cd:81:96:38:ae:5c:a2:f2:c1:df:de:d0:ab:95:
```

```
                    8d:d6:3c:9d:1f:8b:c3:5d:86:2e:5d:f0:b1:72:f5:
                    ab:ac:88:6a:b5:da:b1:22:7b:0b:c8:c8:a5:4b:91:
                    5e:22:13:e9:f9:f5:23:9d:b5:f4:6e:76:ae:ef:ee:
                    a4:3c:c7:c4:c0:59:5c:3f:ab:b3:73:33:26:a6:62:
                    81:61:79:a1:62:f4:6e:88:95:d0:6e:dd:c7:9f:d2:
                    a4:51:11:76:61:ba:70:8a:65:a1:96:16:89:a7:5d:
                    81:d0:44:66:e5:db:56:9e:40:ca:fc:dc:76:24:2e:
                    44:30:00:e5:d6:7d:7b:95:11:d5:58:1d:a3:e8:4f:
                    0b:c9:88:dc:a2:d6:53:99:6c:ca:63:ca:99:6a:9a:
                    92:5e:4c:4d:11:e8:2f:d3:5b:5b:5e:5f:52:a3:73:
                    2d:a5:bb:84:45:0d:8c:19:15:76:cb:08:da:9a:a6:
                    70:15:e8:4d:ec:69:fd:5d:b2:6b:8f:ed:29:51:37:
                    38:8b:c6:46:49:15:94:50:98:b0:f4:68:a4:d7:de:
                    09:71:67:74:9e:77:8c:1d:85:6b:97:ea:e7:5f:45:
                    cc:e0:e6:71:0d:d1:63:00:93:7b:31:98:8e:0b:b4:
                    13:bd:b3:d0:ee:f1:df:21:ee:a9:60:61:ee:37:43:
                    3d:c3
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage: critical
                Digital Signature, Non Repudiation
            X509v3 Subject Key Identifier:
                EE:D9:6B:A9:75:53:CD:4F:EE:1B:4E:19:06:1E:A3:9C:AB:CF:94:FD
            X509v3 Extended Key Usage:
                Code Signing
            X509v3 Authority Key Identifier:
                keyid:25:F8:2B:4B:5D:C8:72:54:AD:E5:F6:A0:2A:17:16:FB:C1:F9:53:81
                DirName:/OU=Copyright (c) 1997 Microsoft Corp./OU=Microsoft
Corporation/CN=Microsoft Root Authority
                serial:6A:0B:99:4F:C0:00:1D:AB:11:DA:C4:02:A1:66:27:BA

            X509v3 CRL Distribution Points:
                URI:http://crl.microsoft.com/pki/crl/products/CodeSignPCA2.crl

            Authority Information Access:
                CA Issuers - URI:http://www.microsoft.com/pki/certs/CodeSignPCA2.crt

    Signature Algorithm: sha1WithRSAEncryption
        38:d9:ef:95:38:9b:5c:98:14:5d:54:6e:69:df:02:c8:e7:b3:
        fb:d3:c2:4d:ad:2f:ab:7f:54:0d:da:32:b6:f8:6a:e6:0d:fb:
        21:1a:77:3e:a5:68:7a:b4:95:7e:8a:5c:f2:43:c4:83:9b:65:
        7d:88:50:51:7c:82:14:f5:83:73:d7:a2:be:5c:ca:02:70:ce:
```

```
        26:6c:17:bc:52:14:a5:89:c0:b7:e4:a1:cc:a1:75:9d:91:71:
        3d:1b:c0:56:00:56:b5:f8:84:26:da:5e:33:fb:d6:25:7a:5e:
        9a:da:a6:fb:f4:f2:41:1a:ac:55:46:ad:48:dc:91:38:13:58:
        09:49:f1:f3:31:87:1f:bc:04:8e:5b:12:65:03:e9:0b:51:d0:
        a1:0c:8a:99:bd:d9:c1:a8:d0:08:15:25:21:b5:b6:57:89:1c:
        d1:5b:86:35:a5:ca:fd:aa:87:ec:a9:37:3f:b7:43:6b:e3:20:
        f1:45:bc:7e:ae:e9:f1:55:b2:a1:48:bc:65:be:53:34:d9:c9:
        e8:06:63:04:06:78:6e:50:ff:48:bb:9b:ea:43:5a:87:db:ad:
        0a:80:f5:59:c5:2c:e4:e5:7f:5b:4a:e5:32:79:ee:22:85:92:
        0c:2d:b3:50:5b:c6:c2:40:58:58:ab:d2:cd:e3:2f:c1:cd:ec:
        6d:9f:37:79

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            0b:72:79:06:8b:eb:15:ff:e8:06:0d:2c:56:15:3c:35
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=Terms of use
at https://www.verisign.com/rpa (c)10, CN=VeriSign Class 3 Code Signing 2010 CA
        Validity
            Not Before: Jun 12 00:00:00 2012 GMT
            Not After : Jun 12 23:59:59 2013 GMT
        Subject: C=CN, ST=Guangdong, L=Guangzhou, O=Guangzhou YuanLuo Technology
Co.,Ltd, OU=Digital ID Class 3 - Microsoft Software Validation v2, CN=Guangzhou
YuanLuo Technology Co.,Ltd
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:c6:ed:0a:22:9b:e6:e7:33:b4:2c:de:15:8a:cf:
                    c7:ef:c0:c5:c5:af:6a:82:97:e7:28:32:38:54:95:
                    2c:4c:55:35:53:8f:74:6e:45:73:6e:0f:38:45:eb:
                    1b:2c:dd:21:46:24:34:47:83:9d:34:3d:47:01:4c:
                    ca:95:52:a3:8c:28:e7:78:1b:7b:1c:76:b2:6c:30:
                    8d:f6:37:b3:63:0b:4d:1e:8a:91:bb:76:d7:30:0d:
                    e6:5e:85:92:9f:d3:f8:46:2d:33:fb:e2:1d:65:59:
                    57:73:73:e2:15:d7:fb:0b:a8:ad:b6:3e:31:ae:df:
                    af:5a:18:55:e6:bd:3c:1c:f4:21:4f:4b:74:26:7c:
                    57:83:37:99:c7:f9:c5:5f:85:1d:fa:14:24:b1:a3:
                    62:f8:fa:a0:27:b5:b9:1b:4e:05:31:dd:a6:28:10:
                    5f:39:72:97:ea:f6:db:eb:b7:9c:37:a6:64:3f:88:
```

```
                9e:9f:13:64:02:d4:77:e1:76:3a:58:3d:71:ca:ae:
                22:7b:b4:63:0d:0a:30:d3:cc:7e:c0:13:66:08:c5:
                c0:cf:5c:b6:44:07:f0:43:34:3e:39:67:1f:11:7c:
                2b:a5:15:87:ce:92:fa:06:f7:5b:87:da:e9:e8:11:
                1d:54:7a:e4:22:84:1c:1b:9f:cf:c7:a3:f2:0d:62:
                2a:cb
            Exponent: 65537 (0x10001)
    X509v3 extensions:
        X509v3 Basic Constraints:
            CA:FALSE
        X509v3 Key Usage: critical
            Digital Signature
        X509v3 CRL Distribution Points:
            URI:http://csc3-2010-crl.verisign.com/CSC3-2010.crl

        X509v3 Certificate Policies:
            Policy: 2.16.840.1.113733.1.7.23.3
              CPS: https://www.verisign.com/rpa

        X509v3 Extended Key Usage:
            Code Signing
        Authority Information Access:
            OCSP - URI:http://ocsp.verisign.com
            CA Issuers - URI:http://csc3-2010-aia.verisign.com/CSC3-2010.cer

        X509v3 Authority Key Identifier:
            keyid:CF:99:A9:EA:7B:26:F4:4B:C9:8E:8F:D7:F0:05:26:EF:E3:D2:A7:9D

        Netscape Cert Type:
            Object Signing
        1.3.6.1.4.1.311.2.1.27:
            0.......
Signature Algorithm: sha1WithRSAEncryption
    8f:d5:34:38:5d:9f:0b:70:5f:d8:46:aa:32:05:6d:10:7b:b2:
    37:de:76:2d:de:f7:46:d6:ab:17:32:95:91:1b:9f:c0:b3:c9:
    93:6f:d5:4d:82:d3:cd:d7:f7:db:64:72:17:9b:f6:08:1b:3e:
    d9:ca:de:49:75:86:44:2d:b2:e6:1f:26:77:28:3b:60:e7:8b:
    93:fc:ea:6a:bc:d1:62:8d:5d:cb:f4:fe:ed:2c:6b:55:10:2d:
    8a:36:cd:cd:0d:56:27:c5:5e:c0:47:f5:d1:1b:7a:a3:23:f9:
    a6:bf:b5:34:74:fa:ad:f4:80:86:b7:46:f8:b8:48:74:0d:5e:
    68:3c:99:31:e6:13:b8:bb:13:cb:5b:69:17:68:60:9b:38:66:
```

```
6a:25:9b:df:a9:6e:62:5b:29:15:91:b1:e8:af:74:59:11:25:
38:ab:5c:b6:2a:33:16:ba:3c:42:76:2c:2b:91:9a:4b:e1:20:
82:4e:b9:91:3f:d5:2c:3b:4e:57:e8:42:a4:37:8c:f6:a3:e2:
7d:6b:b1:27:e2:cf:b5:9b:55:d1:7a:05:50:9b:2e:00:b1:4e:
03:78:dd:52:f9:7d:e3:bc:27:83:63:15:ba:7a:6d:40:b6:40:
42:bd:5a:82:63:30:c8:83:41:95:e0:52:a8:83:51:67:28:c4:
14:2a:d5:db
```

About FireEye

FireEye has invented a purpose-built, virtual machine-based security platform that provides real-time threat protection to enterprises and governments worldwide against the next generation of cyber attacks. These highly sophisticated cyber attacks easily circumvent traditional signature-based defenses, such as next-generation firewalls, IPS, anti-virus, and gateways. The FireEye Threat Prevention Platform provides real-time, dynamic threat protection without the use of signatures to protect an organization across the primary threat vectors, including mobile, Web, email, and files and across the different stages of an attack life cycle. The core of the FireEye platform is a virtual execution engine, complemented by dynamic threat intelligence, to identify and block cyber attacks in real time. FireEye has over 1,100 customers across more than 40 countries, including over 100 of the Fortune 500.

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | info@FireEye.com | www.FireEye.com