Whitepaper:

Alleged APT Intrusion Set: “1.php” Group

zscaler® | ThreatLabZ

Summary

The following release statement provides a brief summary of information related to the "1.php" Group dating from 2008 to present. This Group's methods tend to be spear-phishing emails with malicious PDF attachments or web links to binary executables with a Poison Ivy remote administration tool (RAT) payload. The Group's targeted victims included China/US relations experts, Defense entities, and the Geospatial industry. Zscaler detected repeated infections from this Group to a customer related to this target list. The following report summarizes the incident details to increase awareness of these attacks in order to increase detection, response, and prevention. A much more detailed report has been provided to impacted parties, stakeholders, and other trusted groups dealing with these incidents. The larger report dives into more details about the command and control servers (C&Cs) being used by this Group. If you are working on similar research would like to collaborate, please contact threatlabz@zscaler.com and we will share the detailed report with select entities.

> “This Group's methods tend to be spear-phishing emails with malicious PDF attachments or web links to binary executables with a (RAT) payload.”
>
> -Zscaler ThreatLabZ

> “The Group's targeted victims included China/US relations experts, Defense entities, and the Geospatial industry.”
>
> -Zscaler ThreatLabZ

Introduction

Zscaler provides inline security and policy enforcement of web and email transactions to include full-content inspection and comprehensive transaction logging and analysis. Given that many of Zscaler's customers are large enterprises, it is not surprising that some have been the target of so called Advanced Persistent Threats (APTs). During the course of our daily activities researching various threats, Zscaler ThreatlabZ often uncovers infected hosts that we believe have been compromised via attacks that bear the signature of an APT attack. While there is no universally accepted definition of APT attacks, for the purposes of this paper we will leverage Richard Bejtlich's blog post on the subject[1].

[1] http://taosecurity.blogspot.com/2010/01/what-is-apt-and-what-does-it-want.html

- **Advanced** means the adversary can operate in the full spectrum of computer intrusion. They can use the most pedestrian publicly available exploit against a well-known vulnerability, or they can elevate their game to research new vulnerabilities and develop custom exploits, depending on the target’s posture.
- **Persistent** means the adversary is formally tasked to accomplish a mission. They are not opportunistic intruders. Like an intelligence unit they receive directives and work to satisfy their masters. Persistent does not necessarily mean they need to constantly execute malicious code on victim computers. Rather, they maintain the level of interaction needed to execute their objectives.
- **Threat** means the adversary is not a piece of mindless code. This point is crucial. Some people throw around the term “threat” with reference to malware. If malware had no human attached to it (someone to control the victim, read the stolen data, etc.), then most malware would be of little worry (as long as it didn’t degrade or deny data). Rather, the adversary here is a threat because it is organized and funded and motivated. Some people speak of multiple “groups” consisting of dedicated “crews” with various missions.

> “…the adversary here is a threat because it is organized and funded and motivated. Some people speak of multiple “groups” consisting of dedicated “crews” with various missions.”
>
> -Richard Bejtlich, TaoSecurity blog

Contents

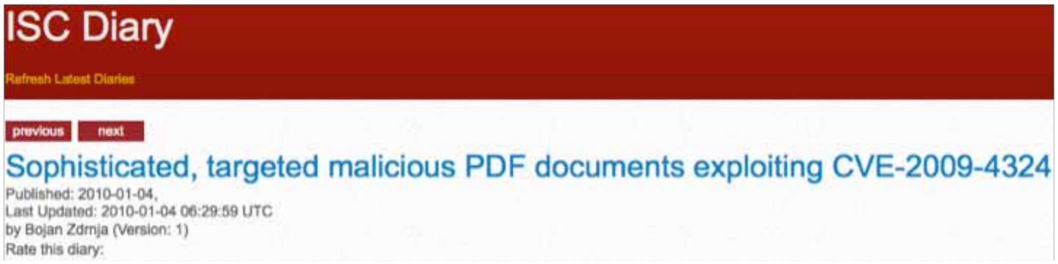
Section 1: "1.php" Group Open-Source Intelligence (OSINT)

There is a good deal of information in the public domain related to "1.php" Group incidents (malware and C&Cs) that can be correlated with incident activity that we identify and detail within this report. Intrusion activities related to this Group date back at least to 2009, if not earlier (there is one sample we found dating back to 2008). For example, a December 7, 2009 blog post by Contagio[2] details a malicious phishing email regarding United States troop deployment in Afghanistan that provides a malicious link to:

File name: WWW.DREAMLIFES.NET/Afghanistan/Afghanistan.zip.
MD5: 052E62513505A25CCFADF900A052709C

Once unzipped, the malware is a Windows executable with an SCR extension that is identified as a Poison Ivy RAT variant. Beyond simple phishing attacks with links to malware, the Group also sends spear-phishing emails with malicious PDF attachments to their targets. For example, the SANS ISC Handler's Diary drew attention to this Group's phishing campaign exploiting CVE-2009-4324 in January 2010. A screenshot of their story headline is below in: Figure 1 SANS ISC Diary Headline related to "1.php" malware campaign[3].

> "Once unzipped, the malware is a Windows executable with an SCR extension that is identified as a Poison Ivy RAT variant."
>
> -Zscaler ThreatLabZ



ISC Diary

Refresh Latest Diaries

previous next

Sophisticated, targeted malicious PDF documents exploiting CVE-2009-4324

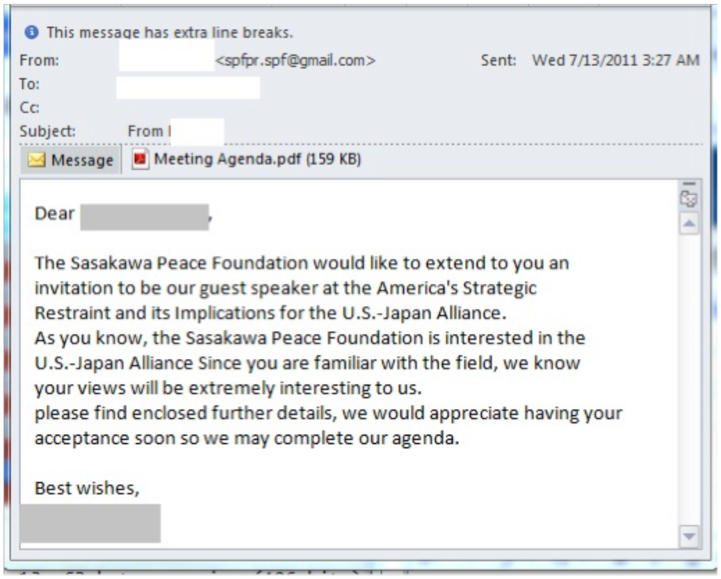
Published: 2010-01-04,
Last Updated: 2010-01-04 06:29:59 UTC
by Bojan Zdrnja (Version: 1)
Rate this diary:

Figure 1 SANS ISC Diary Headline related to "1.php" malware campaign

An example of one of the Poison Ivy RAT payloads used during this campaign was:
File name: SUCHOST.EXE dropped from Request.pdf email attachment
MD5: B0EECA383A7477EE689EC807B775EBBB

[2] http://contagiodump.blogspot.com/2009/12/attack-of-day-poison-ivy-zip-download.html
[3] http://isc.sans.edu/diary.html?storyid=7867

This file received commands from: CECON.FLOWER-SHOW.ORG. More recently, in July 2011, open-source reports[4] exist of Poison Ivy usage surrounding the FLOWER-SHOW.ORG domain. This incident exploited PDF vulnerabilities (CVE-2010-2883) in attached spear-phishing emails targeting experts on Japan, China, Taiwan / USA relationships. See a screenshot of the email in: Figure 2 Spear-phishing email with attachment exploiting CVE-2010-2883.



This message has extra line breaks.

From: [redacted]<spfpr.spf@gmail.com>
Sent: Wed 7/13/2011 3:27 AM
To: [redacted]
Cc:
Subject: From [redacted]

Dear [redacted],

The Sasakawa Peace Foundation would like to extend to you an invitation to be our guest speaker at the America's Strategic Restraint and its Implications for the U.S.-Japan Alliance.
As you know, the Sasakawa Peace Foundation is interested in the U.S.-Japan Alliance Since you are familiar with the field, we know your views will be extremely interesting to us.
please find enclosed further details, we would appreciate having your acceptance soon so we may complete our agenda.

Best wishes,
[redacted]

Figure 2 Spear-phishing email with attachment exploiting CVE-2010-2883

Once the Poison Ivy payload is installed, it frequently uses a unique beaconing pattern to communicate with a C&C server. To illustrate the communication sequence, reference the Joebox sandbox report[5] for the following file:

File name: Halloween.scr
MD5: 5B90896127179F0AD2E6628593CDB60D

[4] http://contagiodump.blogspot.com/2011/07/jul-13-cve-2010-2883-pdf-meeting-agenda.html

This report shows that once infected, the victim:

- Communicates with C&Cs:

    – FREE.COFFEELAUCH.COM (98.126.69.3)

    – FIREHAPPY.SYTES.NET * (98.126.69.3)

- Via HTTP GET requests to the path: /1.php?id=[data1]&id=[data2]&id=[data3]&id=[data4]&id=&id=

    – 2.php, 3.php, and 4.php with id parameters and some with an ending &Done have also been observed

    – The data parameters are information about the infected host (IP, hostname, MAC address, username, and OS/system version) that have been base64 encoded and then XORed. XOR keys of 0x3C and 0x3E have been observed.

> “The “1.php?=” HTTP GET request for the initial C&C check-in has been identified in the majority of past incidents involving this Group and is the reason for the informal “1.php” name used to describe this intrusion set.”
>
> -Zscaler ThreatLabZ

An asterisk following a domain will designate No-IP[6] dynamic DNS domains in this report. Dynamic DNS is a service that provides free, cheap flexible domain hostname to IP address resolution and No-IP is one of the many vendors in this space.

While the malware variants used are generally referred to as Poison Ivy variants, there are many cases of them being detected/labeled as a generic Trojan, Backdoor, or something else entirely. For example, in a December 2009 malware report Kaspersky lists one variant as Trojan.Win32.Buzus.cvdu[7] and in June 2010 another as Trojan.Win32.Agent.eevf[8] .

Note the “1.php?id=” HTTP GET request for the initial C&C check-in. This specific behavior has been identified in the vast majority of past incidents involving this Group and is reason for the informal “1.php” name used to describe these intrusion sets within the report. More information may be garnered from the open-source community, but the above should be a sufficient introduction into the tactics, techniques, and procedures (TTPs) of this Group.

[5] http://support.clean-mx.de/clean-mx/view_joebox.php?md5=9339bb2af4d8c07e63051d0f120530e1&id=679603
[6] http://www.no-ip.com/services/managed_dns/free_dynamic_dns.html
[7] http://www.securelist.com/en/descriptions/7383071/Trojan.Win32.Buzus.cvdu
[8] http://www.securelist.com/en/descriptions/7854148/Trojan.Win32.Agent.eevf

Section 2: Customer Infection Behavior

Zscaler has observed on-going attacks from June 2010 to present, involving a Cleared Defense Contractor. Given the entity involved and the characteristics of the traffic observed, Zscaler believes that the attack is directly related to the “1.php” Group. While these attacks appear related to the “1.php” Group, the beacons do not bear the previously mentioned “1.php” HTTP path. However, there are many similarities regarding these “new” beacons as well as direct relationships regarding previously identified domains and IPs used by the “1.php” group. Presumably, these “new” beacon behaviors have been altered to evade any signatures designed to detect the previous “1.php” beaconing behavior.

> “Zscaler believes that ongoing attacks against a sensitive customer are directly related to the “1.php” Group.”
>
> -Zscaler ThreatLabZ

2.1 GET Beacons with Modified XOR Parameters

One of the first variations that we noticed in the attacks, was that the infected hosts sent HTTP GET request check-ins to URLs with the general pattern of:

FQDN/css.ashx?sc=[data1]&sp=[data2]&ad=[data3]&dh=[data4]&mr=[data5]&tk=

The data parameters contained the same victim information as mentioned in the “1.php” beacons and were also base64 encoded and XORed with a key. Examples of C&Cs that we observed for this particular check-in variant include:

- HOUSE.SUPERDOGDREAM.COM
- HOME.ALLMYDEARFRIENDS.COM
- GOOGLETIME.SERVEIRC.COM *
- INFO.SPORTGAMEINFO.COM
- PEOPLE.ENJOYHOLIDAYS.NET
- PEARHOST.SERVEHALFLIFE.COM *
  (June 2010 – 1st C&C observed in infection)

2.2 GET Beacons with Data moved to URL path

The next variation that we noticed in attacks, involved the infected hosts sending HTTP GET request check-ins to URLs with the general pattern of:

FQDN/[data1]/[data2]/[data3]/[data4]/[data5]

The data did not appear to be XORed in the same manner as the beacons that were previously identified. However, based on size and number of data blocks, it appears that the beacons contain similar information from the victims. Examples of C&Cs used in this infection variant include:

- SATELLITE.QUICKSEARCHMOVIE.COM
- WWW.TOYHOPING.COM
- WORK.FREETHROWLINE.NET
- SEA.ANIMALFANS.NET
- WWW.SEARCHSEA.NET
- LOVE.ANIMALFANS.NET
- WWW.JOBCALL.ORG

> “…it is currently believed that the infection point was through malicious email attachments (as was the case in many of the “1.php” OSINT incidents).”
>
> -Zscaler ThreatLabZ

2.3 HTTPS CONNECTs to C&Cs

The latest variations on these attacks are related to customer infections beginning on August 3, 2011. Prior to infection for this incident, as well as the previous ones listed, web transaction logs did not provide any strong evidence of the infection point – it is currently believed that the infection point was through malicious email attachments (as was the case in many of the “1.php” OSINT incidents). Following infection, many web transactions were witnessed each hour to the C&C servers via HTTPS with the following behaviors:

- CONNECT on port 443/TCP with 200 HTTP response code
- HTTP request version 1.0 with HTTP response version 1.1
- Request size for “keep-alive” beacons were primarily 227 – 228 bytes
- Response size is most commonly between 969 – 990 bytes
- Microsoft Internet Explorer 6.0 user-agent string (hard-coded into malware, as this is not a standard browser for this customer)

Examples of C&Cs used in this infection variant include:

- WWW.SAVAGECOUNTY.NET
- LOOK.CAPTAINSABERTOOTH.NET
- GEOINFO.SERVEHTTP.COM *
- ROSE.OFFICESKYLINE.COM
- WWW.CAREERCHALLENGES.NET
- OFFER.AMERICAMS.N

Section 3: Incident Inter-Relationships

There are a number of domains and IP addresses that have been tied to the previously mentioned incidents. Toward the beginning of the report it was stated that we believed all of these incidents to be related. As has already been seen, there are some similarities across the incidents, such as same victim organization, similar beaconing data blocks, and infection believed to be from malicious email attachments. However, the strongest evidence for their relationship is the fact that related domains and IPs are used for C&Cs across these incidents.

The following Figure 3 - Link-Graph of "1.php" Incident Inter-Relationship provides this illustration with only a small snippet of information from these incidents:

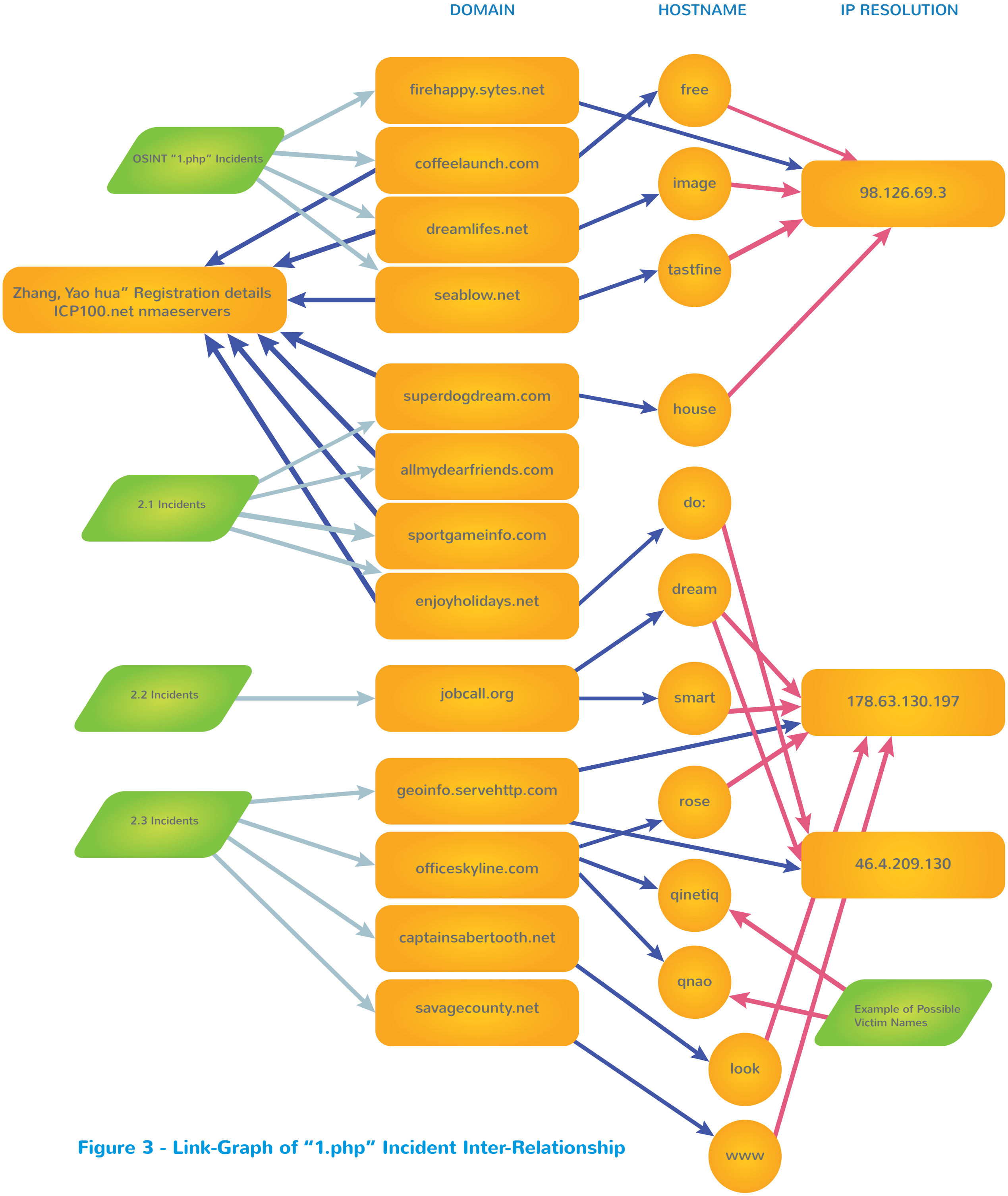


Figure 3 - Link-Graph of "1.php" Incident Inter-Relationship

3.1 Possible Relationship to Other APT Incidents

Past experience with APT-style incidents show that hostnames may be used to identify the C&C for particular victims of interest. For example, in bakerhughes.thruthere.net[9] was a C&C used against Baker Hughes in the disclosed Night Dragon[10] attacks. There have been a number of interesting hostnames used with “1.php” C&C domains that may indicate other potential victims. These hostnames potentially identify victims within the US Government (USG), Defense Industrial Base (DIB), and Geospatial industry. The above link-graph provides one example of such an entity that has information about its attacks already disclosed in the open-source (QinetiQ).

> “There have been a number of interesting hostnames used with “1.php” C&C domains that may include other potential victims.”
>
> -Zscaler ThreatLabZ

“QINETIQ” or “QNAO” (QinetiQ North America Operations) for example, was an HBGary customer. HBGary supported QinetiQ in detection and analysis of on-going targeted attacks against them. Following the Anonymous compromise and leakage of HBGary information, there is significant information in the public domain regarding the attacks against QinetiQ. One such example is *HBGary’s Incident Response Technical Report Supplement* for QinetiQ[11] . Page 8 of that report, in the “History of the strain” section states:

> HBGary has code-named this threat group as “Soysauce”. This group is also known as “Comment Crew” by some, and also as “GIF89a” by some. The choice of codename is completely arbitrary in this context and is simply meant to identify a group of Chinese hackers who have a consistent agenda to target the defense industrial complex.

The name “Comment Crew” and “GIF89a” has been used by researchers because of the behavior of this group to enclose C&C commands within comments on HTML pages or hidden within image files, a technique known as steganography. These indicators have not been witnessed in the attacks previously listed in this report.

Beyond a likely QinetiQ attack relation, there are a number of other hostnames that indicate potential attack targets of the “1.php” Group. Disclosure of other possible victim names is intentionally omitted from this report.

[9] http://hbgary.anonleaks.ch/greg_hbgary_com/2505.html
[10] http://www.mcafee.com/in/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf
[11] http://publicintelligence.info/HBGary-QinetiQ.pdf

Section 4: Lessons Learned

A number of lessons can be learned from analyzing incidents within this intrusion set. In the following section, we will discuss analytical techniques that enterprises should be adopting, in order to uncover similar attacks on their organizations.

4.1 Conduct logging and analytics within your environment

This report shows an evolution of the beaconing behavior from the “1.php” Group. Relying solely on existing signatures of known threats would not have triggered detections. By identifying transactions that are anomalous, it is possible to detect previous or recurring incidents, such as those identified above. Some of the anomalies, which led to the findings in this report, include:

- HTTP version 1.0 requests with version 1.1 responses
- Numerous transactions to an unknown / uncategorized domain
  - Some of these transactions were to No-IP dynamic DNS domains
    - Blocking or heavily monitoring the communication to dynamic DNS domains is recommended
  - Some of these domains were parked
  - Transactions occur during non-standard times (nights / weekends)
  - Some transactions (in particular the GET beacons) had a larger request size than response size
- Microsoft IE 6 user-agent (UA) string usage in an environment that does not typically use this UA

4.2 Correlate with other sources

By leveraging data sources such as passive DNS, domain registration information, other open-source reports, and other research - it is possible to derive information about probable domains and infrastructure used, in other attacks by the same group of attackers. In some cases, this information may provide indicators as to the targets or purpose of the attacks. It should also be noted that making too many assumptions or believing unverified indicators as fact can lead to misleading information. Anyone can set a hostname for a C&C to be “QINETIQ” for example. However, by correlating these domains with a group that has been identified as being involved in APT attacks, provides a stronger indication into their possible target.

> “While the exploitation used in some of the crafted PDF attachments may be considered advanced, for the most part the attack is one of social-engineering.”
>
> -Zscaler ThreatLabZ

4.3 APTs are not always that ‘Advanced’

The above incident reports document (spear-) phishing with a malicious PDF attachment, or link to a binary executable with a Poison Ivy RAT payload. While the exploitation used in some of the crafted PDF attachments may be considered advanced, for the most part the attack is one of social-engineering. This is nothing new and something that other fraudsters / criminals have been leveraging for many years. RSA recently wrapped up their APT summit and their first finding concluded that the “attack vector [is] shifting from technology to people”.[12]

4.4 APTs are not limited to the United States Government or Defense Industrial Base

The victim related to this report is neither a Government agency, nor an entity that would normally be associated with the Defense Industrial Base. While this report does list USG (United State Government) and DIB (Defense Industrial Base) entities as possible victims, there are many more commercial entities within the Geospatial and Telecommunication industries that appear to have been victims of this Group. Zscaler has noted both foreign and domestic entities that have been victims of other APT incidents as well.

[12] http://www.rsa.com/summitresults

4.5 APT Information Disclosure Remains a Challenge

Incident Information Disclosure is an extension to the heated debate around vulnerability information disclosure, and full-disclosure versus responsible-disclosure. Responsible-disclosure is fairly well defined and adopted within the vulnerability space, but it is not within the incident space.

Here are some arguments for “full disclosure” of incident information:

- A larger community of awareness (and thus potential detection possibility), particularly if there are more organizations impacted
- A general philosophy that information should be public and that the Government or information security community should not have secrets kept from the public
- The public should be made aware of which organizations have been victimized so that this information and their response can be weighed before trusting them again in the future

Here are some arguments for “responsible disclosure” (the selective release of information to specific parties) of incident information

- Public release will cause the attacker to alter their TTPs and possibly allow them to make changes to infected systems prior to incident response action, making detection more difficult
- Public release of information can be viewed as attempting to garner the spotlight for financial motives versus genuine concerns about security
- There may be law enforcement (or other) investigations that are on-going and such a release of information could compromise the investigation

Zscaler adheres to the following general principals for incident/vulnerability disclosure:

- Customer specific information is disclosed only to the impacted customer

- Customer information will be redacted prior to public disclosure or disclosure to other impacted parties, stake-holders, and trusted groups within the information security community
- Public disclosure will provide high-level indicators of compromise (such as general network behavior and malicious domains) without the release of specifics as to which organizations were impacted and is done so when it is believed that such information will benefit others in protecting against similar threats
- Based on feedback/approval from the impacted parties, stake-holders, and information security community – additional information may be released to the public

Zscaler is willing to share additional details of the incidents discussed in this report with trusted groups within the information security community to help further their research with regard to similar incidents. If you are interested in sharing data on this and other incidents, we encourage you to contact us at threatlabz@zscaler.com.

Conclusion

By interrogating Zscaler's comprehensive logging repository for anomalous activity and indicators of compromise, a Zscaler ThreatLabZ researcher identified a high-risk entity victimized by a possible APT attack linked to the "1.php" Group. The conclusion that these attacks should be classified as an APT attack are based on the following indicators:

- The victim enterprise is a high risk target, involved in an industry that has regularly been targeted in similar attacks
- Linkages were identified among several previous incidents from 2010 to present, showing persistence
- There remains little to no open-source information on the domains / IPs used in the attack, and the linkage to open-source reports shows a correlation with past APT incidents

- The RAT payload in question is popular among previously documented APT incidents
- Some No-IP dynamic DNS domains used (while a weak APT indicator, dynamic DNS domains have often been used among documented APT incidents, such as Aurora and Night Dragon)
- Hostnames related to victims are used, which is a technique previously documented in other APT attacks
- Nameserver and domain registration information indicates likely Chinese origin of attacks
- VPS/hosting servers used match some of those previously used in alleged APT attacks.

The sum of these indicators has led to our conclusion that this was an attack performed over a significant period of time that focused on a specific target, given the sensitive nature of their work. Based on information in the public domain, it appears that these attacks correlate with others, previously identified as being the work of the “1.php” Group. Identified targets of these attacks include China/US relations experts, USG / DIB entities, and the Geospatial industry. Based on the targets, it is our belief that corporate espionage was the goal of the attacks. Open-source reports suggest that these attacks are more widespread than many realize and that the same or similar actors are compromising numerous organizations in order to steal sensitive intellectual property. As stated within the Lessons Learned section, it is important that those concerned about such attacks be vigilant in their log collection and analysis to identify anomalies or other indications of compromise.

> “The sum of these indicators has led to our conclusion that this was an attack performed over a significant period of time that focused on a specific target, given the sensitive nature of their work.”
>
> -Zscaler ThreatLabZ

About Zscaler: The Cloud Security Company™

Zscaler enforces business policy, mitigates risk and provides twice the functionality at a fraction of the cost of current solutions, utilizing a multi-tenant, globally-deployed infrastructure. Zscaler’s integrated, cloud-delivered security services include Web Security, Mobile Security, Email Security and DLP. Zscaler services enable organizations to provide the right access to the right users, from any place and on any device—all while empowering the end-user with a rich Internet experience.

About Zscaler ThreatLabZ™

ThreatLabZ is the global security research team for Zscaler. Leveraging an aggregate view of billions of daily web transaction, from millions of users across the globe, ThreatLabZ identifies new and emerging threats as they occur, and deploys protections across the Zscaler Security Cloud in real time to protect customers from advanced threats.

For more information, visit www.zscaler.com.