



**X-Force<sup>®</sup> Research and Development Newsletter**

**August 2006**

## There's no such thing as a free lunch with warez...

Fringe content providers, such as those offering illegal software online, are seizing upon the opportunity to distribute malware. For the first half of 2006, a previously non-malicious site, keygen.us, offered Windows Metafile (WMF) exploits which facilitated the installation of malware. Keygen.us had an excellent reputation, despite the nature of its content. While the site no longer hosts WMF exploits, its administrators surely noticed the effectiveness of the WMF vulnerability and considered how much money they might make given their volume of traffic. It is possible that keygen.us' addition to various Web site blacklists caused further diminishing returns over the months beyond the availability of Microsoft's security patch.

Keygen.us is not the norm though. Currently, a number of related Web sites such as crackz.ws, cracks.su, crackinfo.net, and seriall.com all bundle malware with their download offerings. In the case of seriall.com, they do not even bother bundling malware—the only thing they offer is Trojan-Dropper.Win32.Agent.asl regardless of the file name. The others listed are serving up variants of Trojan-Downloader.Win32.Zlob. This scenario is ironic as the end-user is still paying for the software they pirate, just in a circuitous way. The same goes for “free” pornographic content on the Web. Prior to the WMF exploit, these sites still used Web browser exploits to cause the instant installation of Trojan applications such as Porn Dialers, Adware, and Spyware. While a variety of exploits have been in use, the most common two years ago, as well as today, is the MS-ITS exploit (MS04-013).



Looking forward, it is not necessarily the fringe content providers that are the highest risk to the average Internet user. Content-oriented communities such as MySpace are being targeted by a myriad of techniques. This is particularly lucrative with MySpace as it has roughly 54 million unique visitors per month. Consider the case of adware/riskware vendor, Zango. Though it would certainly be illegal for Zango to provide exploit-driven downloads of its software, Zango's activities as they relate to MySpace can be considered exploitation via social engineering.

According to online reports, Zango initially pushed its “Zango Assistant and Search Toolbar” via profiles on MySpace. More recently it was using a sneaky technique involving external movie links that require a special video codec Zango engineered.

Undoubtedly, the only thing special about Zango's codec is what other functionality might be present beyond simply displaying the intended video content. Since video codecs execute natively, they provide an opportunity for non-related code to execute. Even clips that play with one version of the codec can be easily updated to require another version, causing the unwitting user to perpetually be at the mercy of Zango. In the age of complex and misleading end-user license agreements (EULAs), despite the opportunity to decline the Zango software license, users are simply unlikely to comprehend the Zango license or realize that the Zango codec is not offered/endorsed by MySpace.



The question now is how legitimate, online content-oriented communities will react to other firms profiting from their existence, and how they will address individuals attempting to spread malware. One response would be to create new policies to prohibit third party companies from profitable but sketchy activities and apply innovative technologies to keep violations from becoming rampant. With respect to fringe content providers, the future is more certain—as long as there is money to be made with little risk, end-users will continue to be targeted.

-- Robert Freeman, X-Force Adv. R&D Researcher

## Inside the X-Force Engine

### A Closer Look at Skype

Designed by the developers of KaZaa, Skype is a communications application featuring peer-to-peer voice over IP (VoIP), instant messaging, and file transfer. In addition to placing peer-to-peer, client-to-client calls, Skype is also capable of placing calls to and receiving calls from local, as well as international, PSTN (public switched telephone networks) phone numbers.

Significant engineering efforts have made Skype virtually undetectable and therefore ‘unblockable’. This has been done, according to the developers, to prevent competitors and ISPs from blocking Skype

in favor of their own similar VOIP applications. To that end they have been extremely successful.

### Architecture

Skype works according to the following breakdown: Skype network overlay, peer-to-peer registration, encryption, and firewall traversal.

#### Skype Network Overlay

Skype does not rely on a centralized server system in a typical sense. As a peer-to-peer application, it communicates with 'supernodes', which can be other application clients with a public address.

#### Registration and Authentication

In order to function, the application must authenticate and register itself as a client. To do so, Skype communicates with a dynamically generated table of supernodes contained in the registry. The table is a list of address and port pairs that is updated periodically. Once it successfully establishes a connection with a supernode, authentication and registration occurs. Authentication occurs through a number of Skype login servers. Following this, the client may attempt to become a supernode itself.

#### Encryption

The use of encryption is a major component of Skype. It uses RSA with 256 bit AES encryption for data communications and RC4 with a fixed seed for control. Use of public key cryptography, such as RSA, and ephemeral session keys makes Skype almost impossible to tap or decrypt without accessing one of the end clients.

#### Firewall Traversal

Skype can negotiate firewalls in a number of ways. Some firewalls may incorporate network address translation (NAT). Some firewalls may totally block User Datagram Protocol (UDP) or otherwise restrict the client's activities from inside the security perimeter.

With a client behind a NAT firewall, Skype is aware of the client address as well as the external public address of the firewall. When the application starts, channels are established in such a way that other clients are able to connect to the host and request calls or file transfers. In this environment the client cannot become a supernode.

A firewall that restricts access to clients within the network and with the use of a proxy still allows Skype an avenue of communication. When the

application starts, in addition to other initialization, it attempts to open ports 80 (HTTP) and 443 (HTTPS). A host who is also a supernode exposes these ports for additional clients to contact. A client behind a proxy can therefore attempt to contact a supernode on ports used for Web traffic.

### Implications

One major impact that Skype imposes is resource utilization on a network. Because it cannot be blocked, Skype clients have the ability to consume considerable bandwidth even with performance oriented codecs for calls. Network administrators will find this a difficult issue to manage.

Administrators will find enforcing messaging and file transfer policies difficult as well. These features use the same techniques described earlier along with calls. Intellectual property could likely be at risk.

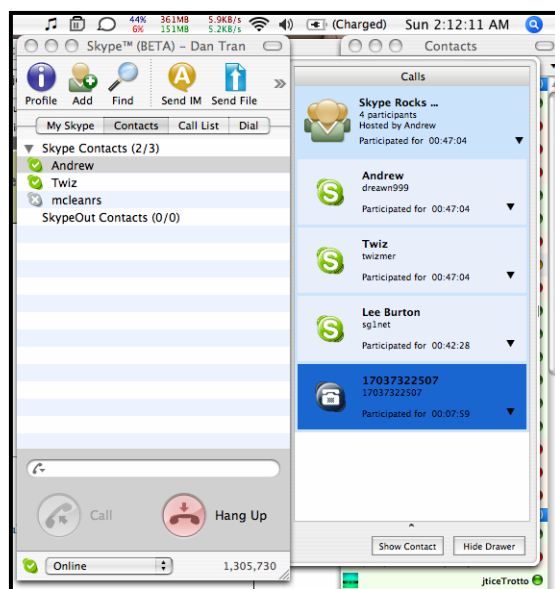
Skype also presents itself as a vector for undetectable backdoors and Trojans. It is possible that unknown flaws and vulnerabilities could be exploited as seen with earlier versions of the application.

### Detection

Given the extensive use of encryption and peer-to-peer technologies, it is extremely difficult at this time to reliably detect and block Skype on a network. However, when the application starts, it will attempt to call in to determine if there are program updates available. It is possible to detect a host running the application based on this request. Unfortunately, this is not guaranteed since the option to request updates can be disabled. The option is on by default. Internet Security Systems' Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) products have detection for this with HTTP\_Skype.

It is also possible to detect the initial response from a supernode when the connection request is UDP. This method cannot be used when the client is behind a restricted firewall preventing UDP requests. ISS is planning on adding this method of detection to its protection products in an upcoming update. However, Skype cannot be blocked this way since a failure to properly connect via UDP forces it to use TCP exclusively.

While the Skype client could be detected by way of the running process or the registry keys on Windows,



versions exist for Macintosh and Linux. The Skype protocol has reportedly been reverse-engineered by a group in China, therefore it is possible that before too long, additional Skype clients may appear.

#### Additional references

[http://www.rootsecure.net/content/downloads/pdf/skype\\_protocol.pdf](http://www.rootsecure.net/content/downloads/pdf/skype_protocol.pdf)

-- Scott Warfield, X-Force Protection Engineer

## Protection Corner

### What is Coverage?

It happens all the time. Someone releases an advisory for a newly discovered critical-risk vulnerability and every security vendor on the planet races to provide coverage. Organizations rely on security vendor's coverage for protection from potential attacks. Once the update is installed, the organizations observe a new line item in their protection policy, they check the checkbox, and sleep soundly. But what did these organizations really do to protect themselves? In some cases, these actions are enough. But other times, organizations only enable a signature that is worth no more to them than the text in the policy itself.

This is fast becoming the nature of enterprise security management—checking off the appropriate line items. Too often, very little attention is paid to whether that line item in a policy is actually doing anything constructive to provide protection. It is an attitude that needs to change; having worthless signatures is just that—worthless. How can enterprise security vendors justify this kind of 'protection' to their customers? Thankfully, Gartner is now starting to consider signature quality when it evaluates solutions for its Magic Quadrant. Hopefully, in the future, Gartner may actually be equipped to verify protection quality and robustness.

Below are examples of vulnerabilities that legacy IDS/IPS solutions struggle to properly cover. In each case, irresponsible signature-based vendors claimed to provide coverage for the issue.

#### Example 1:

On January 10, 2006, eEye released an advisory for a stack-based buffer overflow in Apple's QuickTime Player (<http://www.eeye.com/html/research/advisories/AD20060111c.html>).

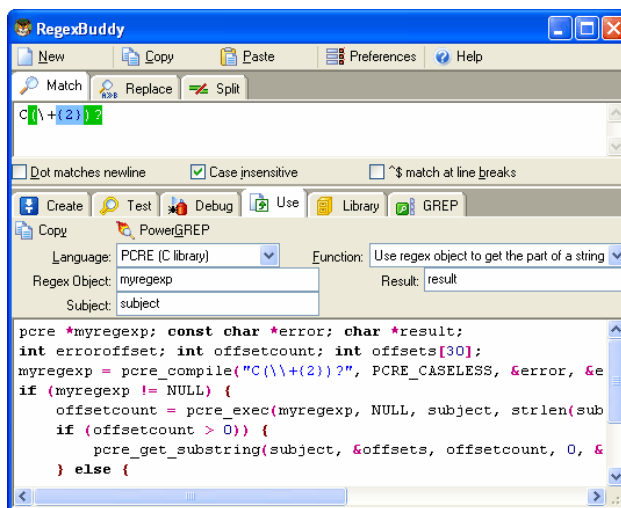
This was the result of handling malformed QuickTime Image Files (QTIF). What eEye failed to notice is that QTIF is simply a wrapper for other file types. In fact, the vulnerability is actually in the JPEG handler in QuickTime. This is why the X-Force

Database write-up on this issue falls under the title "Apple QuickTime JPEG Image Buffer Overflow" (<http://xforce.iss.net/xforce/xfdb/24054>).

While most IDS/IPS vendors were looking for malicious QTIFs, the X-Force parsed the QTIF looking for a wrapped JPEG, passed the JPEG off to the JPEG parser, and looked for the vulnerable condition.

The real problem in this case is that the vulnerability occurs when the individual bytes of a 16 byte table are summed and are greater than the size of a static-sized stack buffer. This sum is used to determine how much data following the table should be copied into the stack buffer. Proper detection requires the ability to sum the value of 16 bytes. But it is impossible to do a summation in a basic Perl compatible regular expression (PCRE) engine. Vendors would effectively have to create one PCRE for every combination of 16 bytes that would sum to larger than the affected value. In this case, the number of PCREs is in the billions of billions of billions.

Even with that impossibility, many PCRE-based IDS/IPS vendors claim coverage. It begs the question, "What, then, is coverage?"



#### Example 2:

On June 13, 2006, the Zero Day Initiative released an advisory on a heap-based buffer overflow in MSHTML.dll that was the result of improper handling of five and six byte encoded UTF-8 characters (<http://www.zerodayinitiative.com/advisories/ZDI-06-017.html>).

UTF-8 is a character encoding that allows characters to be represented by 2, 3, 4, 5, or 6 bytes. The first few bits of the first byte of the character tell the application rendering the text what type of encoding is being used. This must be checked for each character as it is encountered in the character stream. X-Force researchers were able to determine that there are dozens of combinations of three

character groupings that, when encoded in specific ways, would lead to the heap overflow condition. For example, if Internet Explorer were to encounter a five-byte encoded character followed by two three-byte encoded characters, this could lead to the vulnerable condition.

When reviewing the effectiveness of several IDS/IPS vendors' coverage for this issue, X-Force found that some of them only covered one of the encoding combinations. To make matters worse, they look for specific characters, not just the encoding method used. This is a case where PCRE would have afforded them all they needed to create proper signatures. Other IDS/IPS vendors simply lacked the research capability to determine how to accurately detect this issue.

### The Future

Moving forward, we must all work to change the industry's perception of coverage for vulnerabilities. A line item in a policy does nothing to guarantee actual protection for a particular vulnerability. In many cases, legacy IDS/IPS signatures simply catch the individual proof-of-concept the vendor was able to download, or one they purchased.

In this short article, X-Force has demonstrated two cases in which looking for an individual exploit still leaves systems vulnerable to billions of permutations. Furthermore, hundreds of new vulnerabilities are discovered each month that require skilled researchers to investigate, or are difficult to handle using a PCRE engine. Only the X-Force keeps you ahead of the threat, unlike PCRE-dependent vendors that focus only on being "ahead of the customer."

-- David Dewey, X-Force Adv. R&D Researcher

## A Month in Review

Below is a brief summary of security content developed or processed in the month of July 2006.

### Malcode:

In July, the X-Force alpha-testing platform for the Virus Prevention System (VPS) engine (codename Catfish) identified 7 Zero-Day malcode outbreaks, six of which are Downloader Trojans and one of which is a Password Stealer.

- Most of the Downloader Trojans were simple Downloaders whose sole purpose was to download and install additional malcode on the affected systems. Most of the Downloaders were received July 19 -23.
- In the middle of July, a new variant of the W32.PWS.Goldun family of password-

stealing (Trojans which installs a malicious BHO on the system) was discovered.

- On July 23 a new variant of the Goldun family was spammed, but instead of the Password Stealer being spammed, a Downloader which retrieves the main Password Stealer was spammed (W32.Downloader.Goldun.DJ). This Downloader was later reported in the SANS ISC:  
<http://isc.sans.org/diary.php?storyid=1507>

### Sample Harvesting:

It is worth noting that as part of X-Force's continued work to strengthen ISS antivirus, anti-spyware and anti-malware protection, we investigated and added another 50,283 new samples to our malcode zoo this month. That's a lot of malware in one month!

### Vulnerabilities:

Last month also saw 582 new vulnerabilities disclosed and analyzed by X-Force. This represents a 42 percent increase over the same seven month period last year, and a 49 percent increase over July 2005.

	Reported				Total
	Critical	High	Medium	Low	
Apr	3	120	330	129	582

Of these vulnerabilities, 528 were remotely exploitable, 66 could only be exploited locally and 12 could potentially be exploited both remotely and locally.

Vulnerability Breakdown	
<b>Bypass Security</b>	<b>26</b>
An attacker can bypass security restrictions such as a firewall or proxy, an IDS system or a virus scanner.	
<b>Data Manipulation</b>	<b>66</b>
An attacker is able to manipulate data stored or used by the host associated with the service or application.	
<b>Denial of Service</b>	<b>89</b>
An attacker can crash or hang a service or system or take down a network.	
<b>File Manipulation</b>	<b>10</b>
An attacker can create, delete, read, modify or overwrite files.	
<b>Gain Access</b>	<b>295</b>
An attacker can obtain local and remote access. This also includes vulnerabilities by which an attacker can execute code or commands, because this usually allows the attacker to gain	

access to the system.

**Gain Privileges** **27**

Privileges can be gained on the local system only.

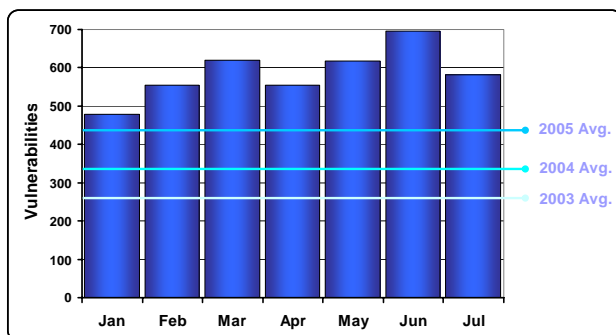
**Obtain Information** **69**

An attacker can obtain information such as file and path names, source code, passwords or server configuration details.

**YTD Total** **4105**

\* Right-hand column represents unique vulnerability count

### Vulnerabilities per Month vs. Yearly Average



### Top 5 Vulnerable Vendors of the Month

Oracle	<b>65</b>
Microsoft	<b>55</b>
Mozilla	<b>14</b>
Cisco	<b>9</b>
OpenCMS	<b>9</b>

\* Right-hand column represents unique vulnerability count

### X-Force Security Content:

In July, X-Force added 28 new events for various vulnerabilities, delivered three Level-0 X-Press Update® (XPU) product enhancements related to the Microsoft Super-Tuesday patches, and added six new blocking responses.

#### Updated Protocol Parsers:

- HTTP format string detection
- SSL
- SMB
- Veritas

#### Updated Content Parsers:

- Html
- Javascript
- Biff
- Compound file support( doc, xls, ppt, etc)

#### New Protection Decodes:

- SMB\_PIPE\_Invalid\_Ptr\_Corruption

- HTTP\_Httpunnel\_Detected
- Oracle\_AuthAlterSession\_SqlExec
- Veritas\_NetBackup\_VolumeMgr\_Sscanf
- PE\_ClamAV\_PE\_UPX\_Overflow
- Scada\_ICCP\_Long\_TPDU
- HTTP\_ASP\_AppFolder\_Disclosure
- HTTP\_MhtmlMid\_Bo
- HTML\_ASP\_Malformed
- URL\_File\_URI\_Overflow
- MSRPC\_RRaS\_Reg\_BO
- SMB\_MailSlot\_Heap\_Overflow
- DHCP\_Large\_Option\_Bo
- CompoundFile\_Excel\_Unspecified\_BO
- CompoundFile\_Excel\_HLink\_BO
- CompoundFile\_Excel\_CollInfo\_BO
- CompoundFile\_Excel\_Object\_BO
- CompoundFile\_Excel\_FNGroupCount\_BO
- CompoundFile\_Excel\_Label\_BO
- CompoundFile\_Excel\_GIF\_Malformed\_Size
- CompoundFile\_Excel\_Sheet\_Malformed\_Size
- CompoundFile\_Word\_HLink\_BO
- BIFF\_Workbook\_Selection\_Overflow
- CompoundFile\_Excel\_Selection\_BO
- Image\_GIF\_Malformed\_Size
- Image\_PNG\_Zlib\_Bo
- LDAP\_Modify\_Req\_Bo
- Backup\_Invalid\_Input

#### New Blocking for:

- SMB\_PIPE\_Invalid\_Ptr\_Corruption
- NNTP\_List\_Response\_Overflow
- MSRPC\_MSRTC\_Message\_GUID\_BO
- MSRPC\_RRaS\_Reg\_BO
- MSRPC\_RRaS\_BO
- DHCP\_Large\_Option\_Bo