

# Blackhat Hacking

---

How to hack and not get caught

Brady Bloxham  
Silent Break Security  
[brady@silentbreaksecurity.com](mailto:brady@silentbreaksecurity.com)

# Overview

---

What is OpSec?

Methodology

TTPs (Tactics, Techniques, and Procedures)

Conclusion



What is OpSec?

---

# What is OpSec?

---

## First things first

- Examine your activities from an adversary's point of view
- Way of life
- NOT a set of rules
- Best of all...it's free!

Above all → Shut Your Mouth

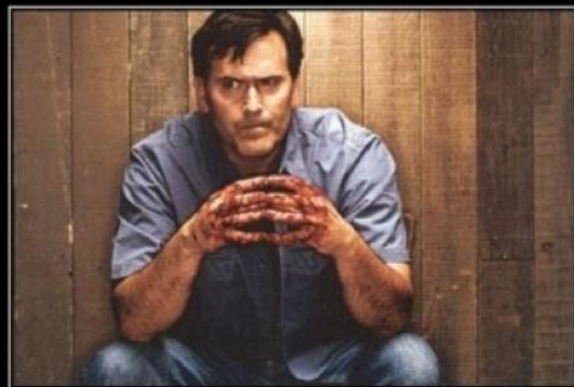




# What is OpSec?

---

- Proactive paranoia
  - It doesn't work retroactively!



**PARANOIA**

I don't trust a single one of you What-ops

**I USED TO BE  
PARANOID  
BUT NOW I KNOW  
THEY'RE OUT  
TO GET ME!**



**STAY  
PARANOID  
AND  
TRUST  
NO ONE**

# What is OpSec?

---

Stay paranoid...and cover your webcam!





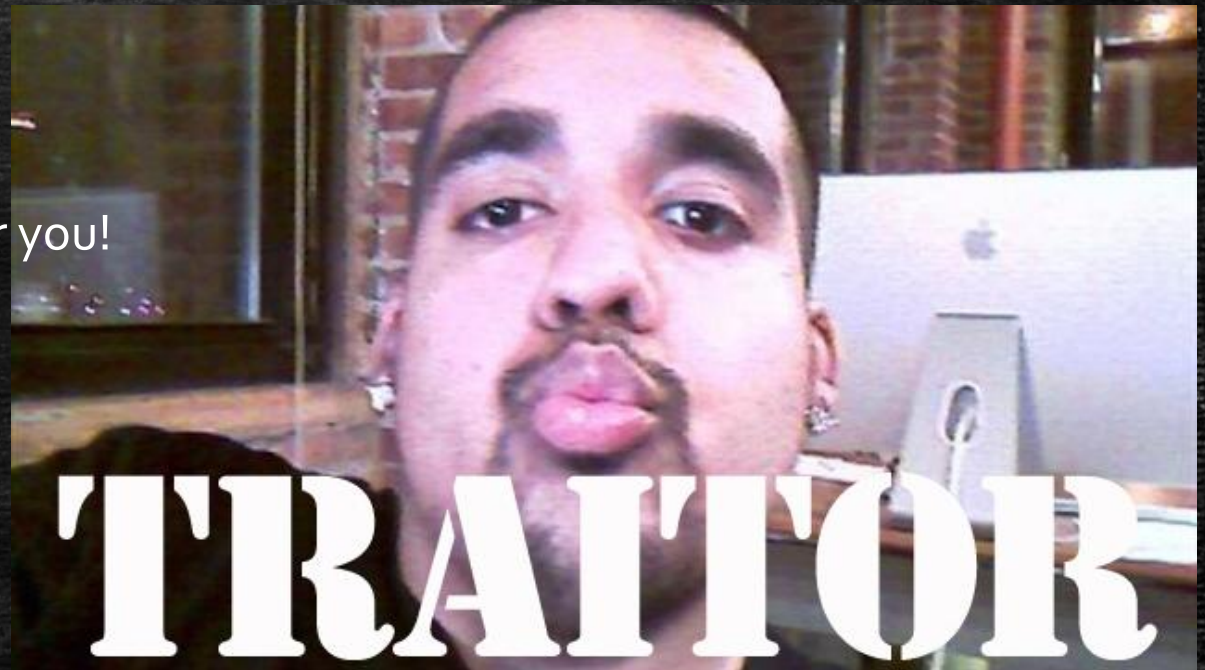
# What is OpSec?

---

Work alone

Avoid being blackmailed

No one is going to jail for you!



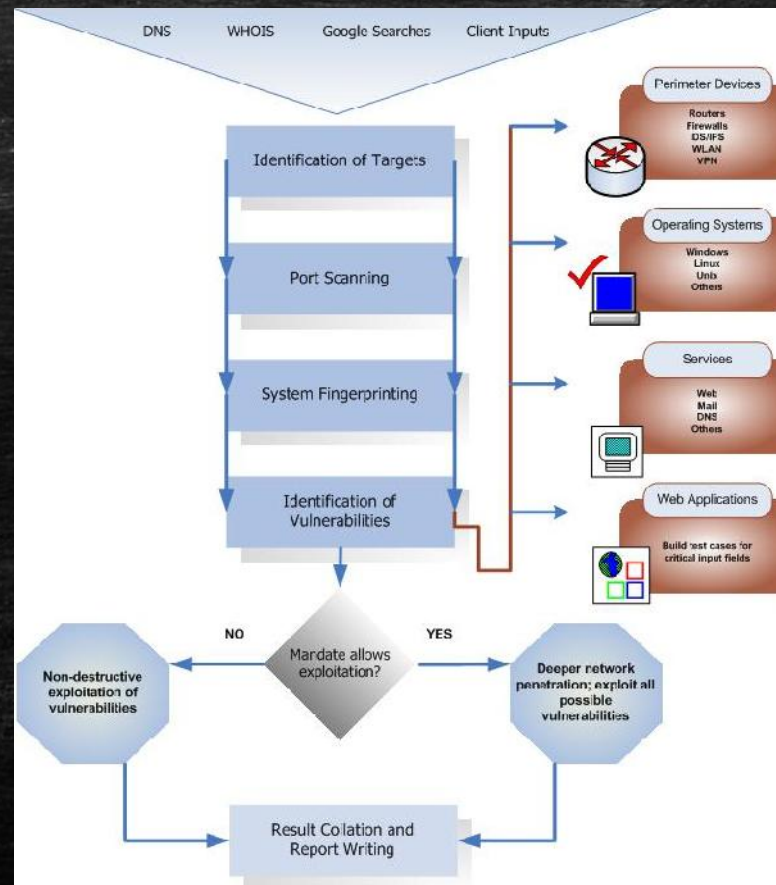
# Methodology

---



# Methodology

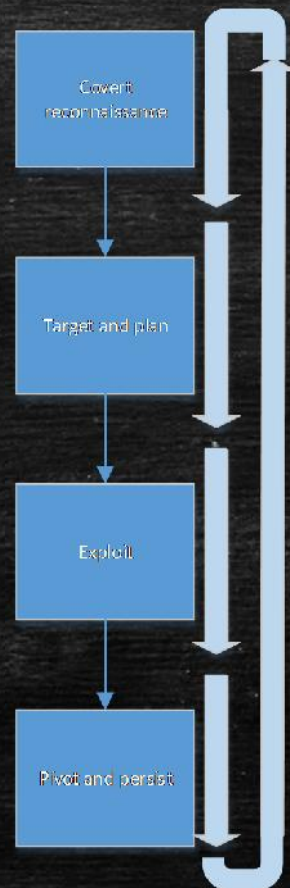
## The Old Way



# Methodology

---

## The New Way





# Methodology

---

## Money trail




- PATRIOT Act
- Various types
  - Pre-paid credit cards
  - Pre-paid credit cards + Paypal
  - Western Union
  - Bitcoin
    - Not truly anonymous!
    - Every transaction is publically logged
    - So...use bitcoin mixing/eWallet



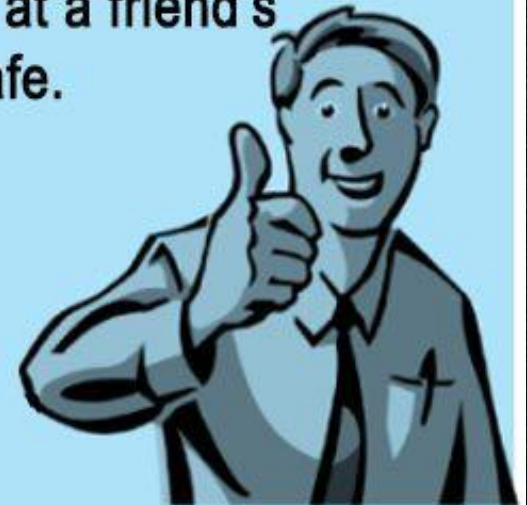
# Methodology

---

## Covert Infrastructure

- VPS   
Careful of payment
- TOR   
Slow
- VPN  
Torguard.net  
Btguard.com
- Create your own!    
SOHO routers  
Hack onto other servers

They said don't try this at home...  
So I'm gonna try it at a friend's  
house just to be safe.





# Methodology

- Covert Infrastructure

## Search

<< prev 1 2 3 4 5 >> next

Date D A V Description

2013-03-22	↓	-	🔍	TP-Link TL-WR740N Wireless Router - Denial Of Service Exploit	4363	hardware	LiquidWorm
2013-03-19	↓	-	🔍	Wireless Router MI424WR-GEN3I - CSRF Vulnerability	3539	hardware	Jacob Holcomb
				408 (ADSL Router) Authentication Bypass	3373	hardware	Ivano Binetti
				D UniteHostRouter Buffer Overflow	705	windows	metasploit
				orks ADSL2/2+ Wireless Router ASL-26555 Password Disclosure	1118	hardware	Alberto Ortega
				Wireless Router Password Disclosure	3426	hardware	Avinash Tangirala
				ter Denial of Service	7233	hardware	PoURaH
				2604 CSRF Vulnerability (ADSL Router)	2029	hardware	KinG Of PiraTeS
				408 (ADSL Router) CSRF Vulnerability	6586	hardware	Ivano Binetti
				A UniteHostRouter <= 3.8.2 Remote Pre-Auth Command Execute	2476	windows	Abysssec
				ter 4200 and 4300 Command Execution	1334	hardware	metasploit
				uter CT-5624 Remote Root/Support Password Disclosure/Change Exploit	3446	hardware	Todor Donev
				r Fast 3304/3464/3504 Telnet Authentication Bypass	5985	hardware	Elouafiq Ali
				s SMTP router, EMAIL server and client DoS	2261	multiple	unknown
				less Router FS07234-4 v5 Exploit	4847	hardware	Aodruez
				SL Router CT-5367 C01_R12 Remote Root	16379	hardware	Todor Donev
				itation	6328	hardware	FX
				sys Router CSRF Vulnerabilities	1766	hardware	Martin Barbella
				nk Router Models Authentication Bypass Vulnerability	3408	hardware	Craig Heffner
				84GA Router CSRF + Persistent XSS Exploit	1125	hardware	I3D

Results 1 - 10 of about 98445 for WR740N



113.237.209.0  
China Unicom Liaoning  
Added on 30.05.2013

🇨🇳 Shenyang

Details

HTTP/1.0 401 Unauthorized

Server: Router

Connection: close

WWW-Authenticate: Basic realm="TP-LINK Wireless N Router **WR740N**"

Content-Type: text/html



60.31.98.8  
China Unicom Neimeng  
Added on 30.05.2013

🇨🇳 Baotou

Details

HTTP/1.0 401 Unauthorized

Server: Router

Connection: close

WWW-Authenticate: Basic realm="TP-LINK Wireless N Router **WR740N**"

Content-Type: text/html

### Login Incorrect

80.91.65.246  
Wireless Communication S.L.  
Added on 30.05.2013



Details

HTTP/1.0 401 N/A

Server: Router Webserver

Connection: close

WWW-Authenticate: Basic realm="TP-LINK Wireless Lite N Router **WR740N**"

Content-Type: text/html

Celebrating 3  
years of  
Shodan

# Methodology

---

## Don't be a hoarder

- Principle of least use
  - Don't collect what you don't need
  - Don't hoard data
  - Delete it when you're done
- Be smart about it
  - Dedicated infrastructure
  - Truecrypt containers
  - VMs with snapshots
  - Qube-OS



# EXCESSIVE HOARDING

You do NOT need that many pizza boxes



TTPs (Tactics, Techniques, and Procedures)

---

# TTPs

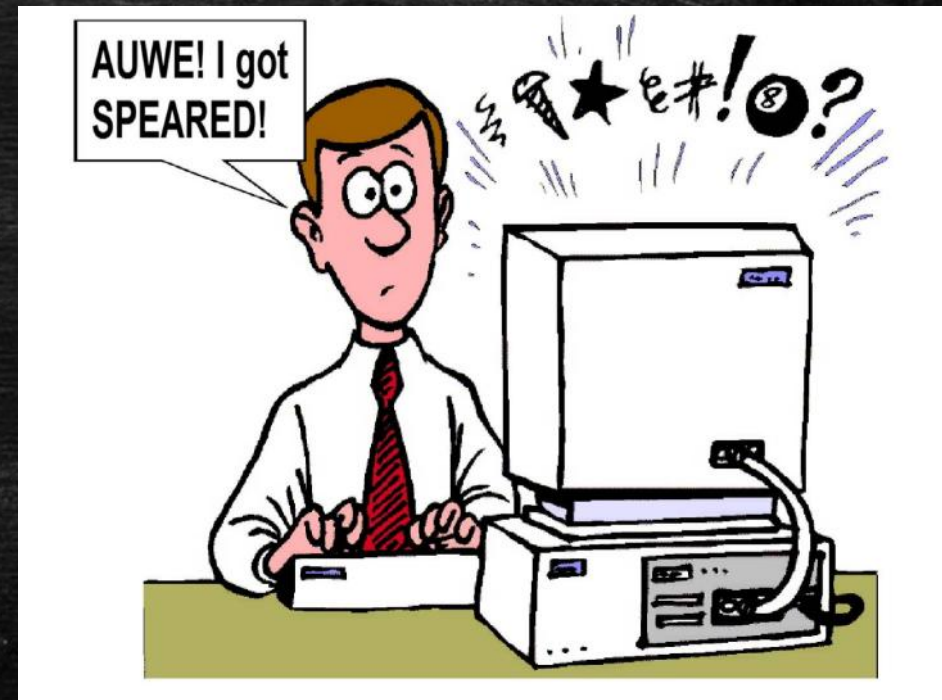
## Spear phishing

- Click rate ~ 25-35%



## Countermeasure

- End user training but...it should reflect current threat environment.
- Configure spam filter!
- Use proxy to block!





# TTPs

## LinkedIn

Scooby Doo requested to add you as a connection on LinkedIn:

Shaggy,

I'd like to add you to my professional network on LinkedIn.

- Scooby Doo

Accept

[View invitation from Scooby](#)

### WHY MIGHT CONNECTING WITH Scooby Doo BE A GOOD IDEA?

Scooby's connections could be useful to you

After accepting the invitation, check Scooby's connections to see who else you may know and who you might want an introduction to. Building these connections can create opportunities in the future.

© 2012, LinkedIn Corporation



PayPal Email ID [REDACTED]

Dear [REDACTED],

On Jan. 2013, your credit card has been removed from your paypal account.

Possible removal reasons:

- Your card has been declined.
- Your card has expired.
- Your card has insufficient funds to cover transactions.

To avoid any service interruption, please Add a New Card by following the steps below. If you do not:

You may no longer be able to send instant payments using PayPal.

To Add a New Card, click on the link below:

[Add a New Card](#)

**Dangerous link  
Do NOT click.**

After you Add a New Card, you can send money quickly and easily, accept unlimited credit card and bank account payments, use special tools for sellers, and receive Customer Service hotline help 7 days a week. You can also receive payments for low fees.

PayPal ? The safer, easier way to pay

- Make sure your money is there when you need it.
- Accept credit cards and checks wherever your customers are with PayPal Here.

Fight fake emails

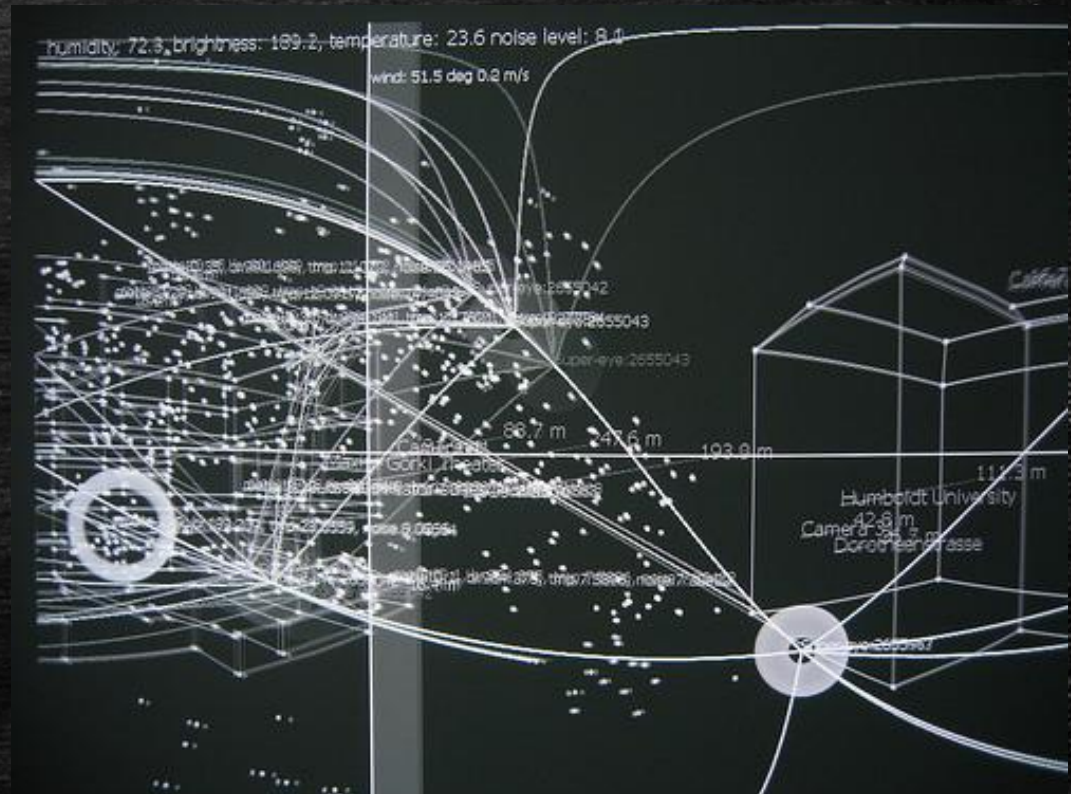
- Forward suspicious emails to spoof@paypal.com.
- Make sure you're using the latest internet browser.
- Visit the PayPal Security Center.

# TTPs

Pop and pivot!

Be strategic!

- Don't pop...just to pop
- Find high value targets
  - Tasklist of remote systems
  - Net use for remote dir of c:\Users
  - Query AD for logon events





# TTPs

---

“Work” during the day

- Blend in with the noise
- Harder to filter logins
- Easier to identify key targets

## Countermeasures

- Monitor, monitor, monitor...especially privileged accounts
- Create user accounts for domain admins



## Steroids

Help you blend in with the crowd

# TTPs

---

## Cover your tracks

- Clean the logs
- Watch the prefetch
- Registry MRUs
- Change time stamp!
- Remove tools!



$\text{Risk} = \text{Threat} \times \text{Vulnerability} \times \text{Cost}$

- The best way to not get caught, is to not leave tracks.



# TTPs

## MRUs

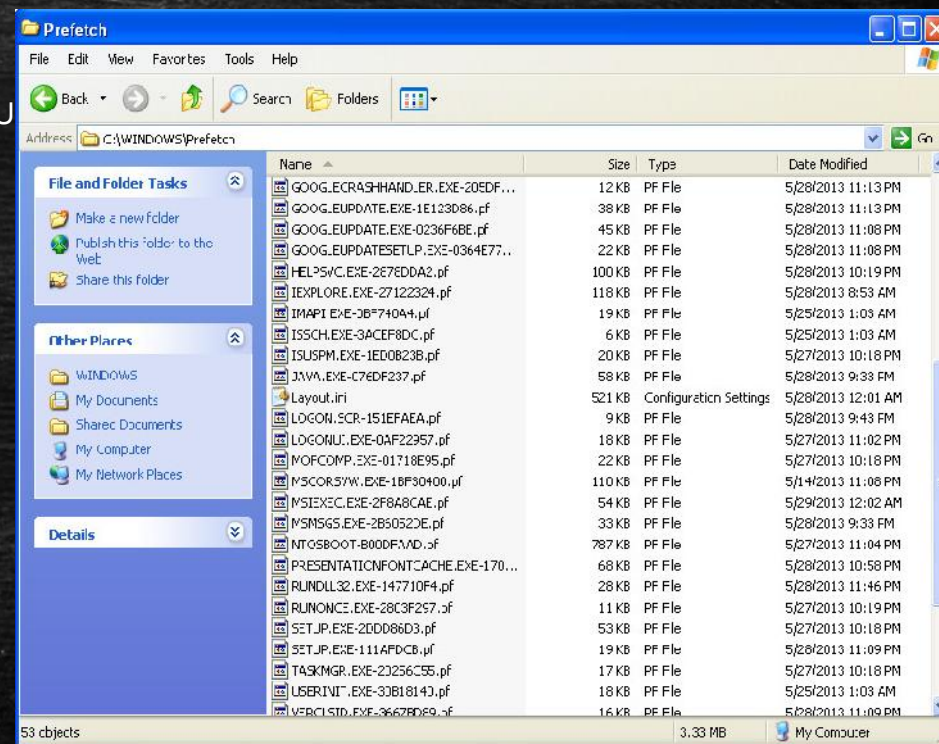
- HKCU\SW\Microsoft\Windows\CurrentVer\Explorer\FindComputerMRU
- HKCU\SW\Microsoft\Windows\CurrentVer\Explorer\PrnPortsMRU
- HKCU\SW\Microsoft\Windows\CurrentVer\Explorer\RunMRU
- HKCU\SW\Microsoft\Windows\CurrentVer\Explorer\StreamMRU

## Audit Policy

- HKLM\Security\Policy\PolAdtEv

## Clean Logs

- Windows Defender
  - Binary logs! Check out MPDetection.txt
- McAfee
  - BufferOverflowProtectionLog.txt
  - AccessProtectionLog.txt
- Symantec
  - \Docume~1\AllUse~1\Applic~1\Symantec\Symantec Endpoint Protection\Logs



# TTPs

---

Test, test, test, test, test, test, test, test, test, test, test, test, test

Modifying the target is for noobs

- Modify your tools instead
- Packers, crypters, modifying the source, etc., etc.

want to know more?

use the source, Luke!







SHA256: 0f6febd5c2030f70036b458cbd396ae63de3454497161b7c5afae3ccfea0a2e8

File name: msf.exe

Detection ratio: 35 / 44

Analysis date: 2012-10-30 06:54:10 UTC ( 0 minutes ago )



More details

Analysis Comments Votes Additional information

Antivirus	Result	Update
Agnitum	Trojan.Rosena.Gen.1	20121029
AhnLab-V3	Trojan/Win32.Shell	20121029
AntiVir	TR/Crypt.EPACK.Gen2	20121030
Antiy-AVL	-	20121027
Avast	Win32:SwPatch [Wrm]	20121029
AVG	Win32/Heur	20121030
BitDefender	Backdoor.Shell.AC	20121030
ByteHero	-	20121029
CAT-QuickHeal	Trojan.Swrort.A	20121030
ClamAV	-	20121029
Commtouch	W32/Swrort.A.gen!Eldorado	20121030
Comodo	TrojWare.Win32.Rozena.A	20121030
DrWeb	Trojan.Swrort.1	20121030
Emsisoft	Backdoor.Shell.AC (B)	20121030
eSafe	-	20121028



SHA256: c2c66b7c7f18cab0ca98305611ffca238d9298599db7ddb7a2311f9ca55ca538

File name: msf1.exe

Detection ratio: 28 / 44

Analysis date: 2012-10-30 06:56:18 UTC ( 0 minutes ago )



More details

Analysis Comments Votes Additional information

Antivirus	Result	Update
Agnitum	Suspicious!SA	20121029
AhnLab-V3	-	20121029
AntiVir	HEUR/Crypted	20121030
Antiy-AVL	-	20121027
Avast	-	20121029
AVG	Win32/Heur	20121030
BitDefender	Backdoor.Shell.AC	20121030
ByteHero	-	20121029
CAT-QuickHeal	(Suspicious) - DNAScan	20121030
ClamAV	-	20121029
Commtouch	W32/Threat-HLLIM!Eldorado	20121030
Comodo	Packed.Win32.Packer.~GEN	20121030
DrWeb	-	20121030
Emsisoft	Backdoor.Shell.AC (B)	20121030
eSafe	Win32.Stration	20121028





SHA256: 0e68c115a642d67100511a3d3870d3a03aedd9fd309cb9e65bab53a5580df2f0

File name: msfExe.exe

Detection ratio: 2 / 44

Analysis date: 2012-10-30 07:29:14 UTC ( 0 minutes ago )



More details

Analysis Comments Votes Additional information

Antivirus	Result	Update
Agnitum	-	20121029
AhnLab-V3	-	20121029
AntiVir	-	20121030
Antiy-AVL	-	20121027
Avast	-	20121029
AVG	-	20121030
BitDefender	-	20121030
ByteHero	-	20121029
CAT-QuickHeal	-	20121030
ClamAV	-	20121029
CommTouch	-	20121030
Comodo	-	20121030
DrWeb	-	20121030
Emsisoft	-	20121030
eSafe	-	20121028

# TTPs

---

## Environmental awareness

- Network
  - SYN vs Connect scan
  - ping -n 1 <ip>
  - SSL where possible
- System
  - Avoid domain accounts
  - Build a profile

## Countermeasures

- Create baselines (SIEM, netflow, etc.)
- Don't ignore anomalies or alerts



(As far as we know, photo is public domain)



# TTPs

---

## Data exfiltration techniques

- Archive files (usually .rar)
- Stage on separate box
  - Recycle bin
  - System volume information

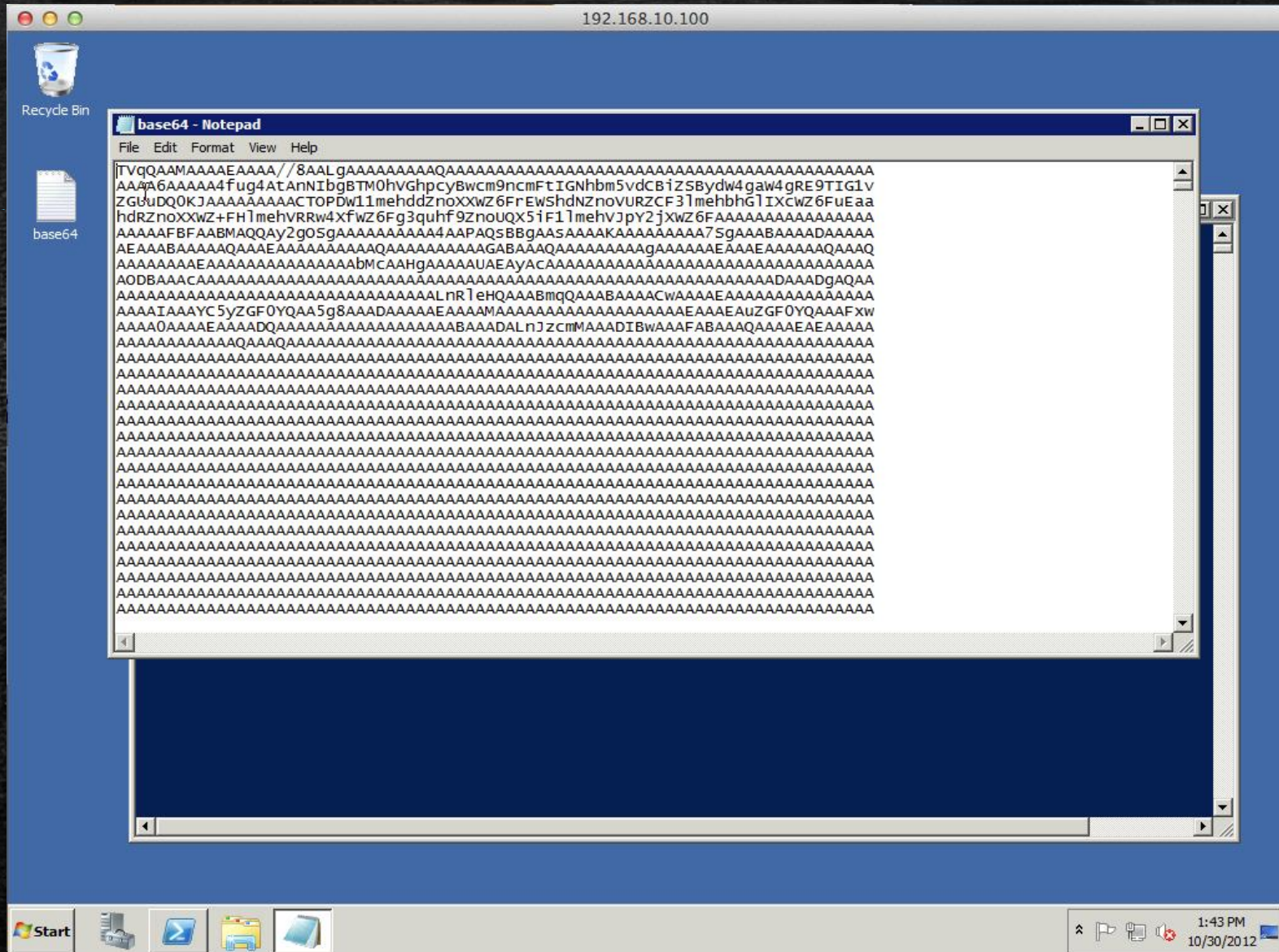
## Data exfiltration channels

- Compromise server in the DMZ
- Transfer via RDP
- Base64 en/decode to/from target via shell
- HTTP/S

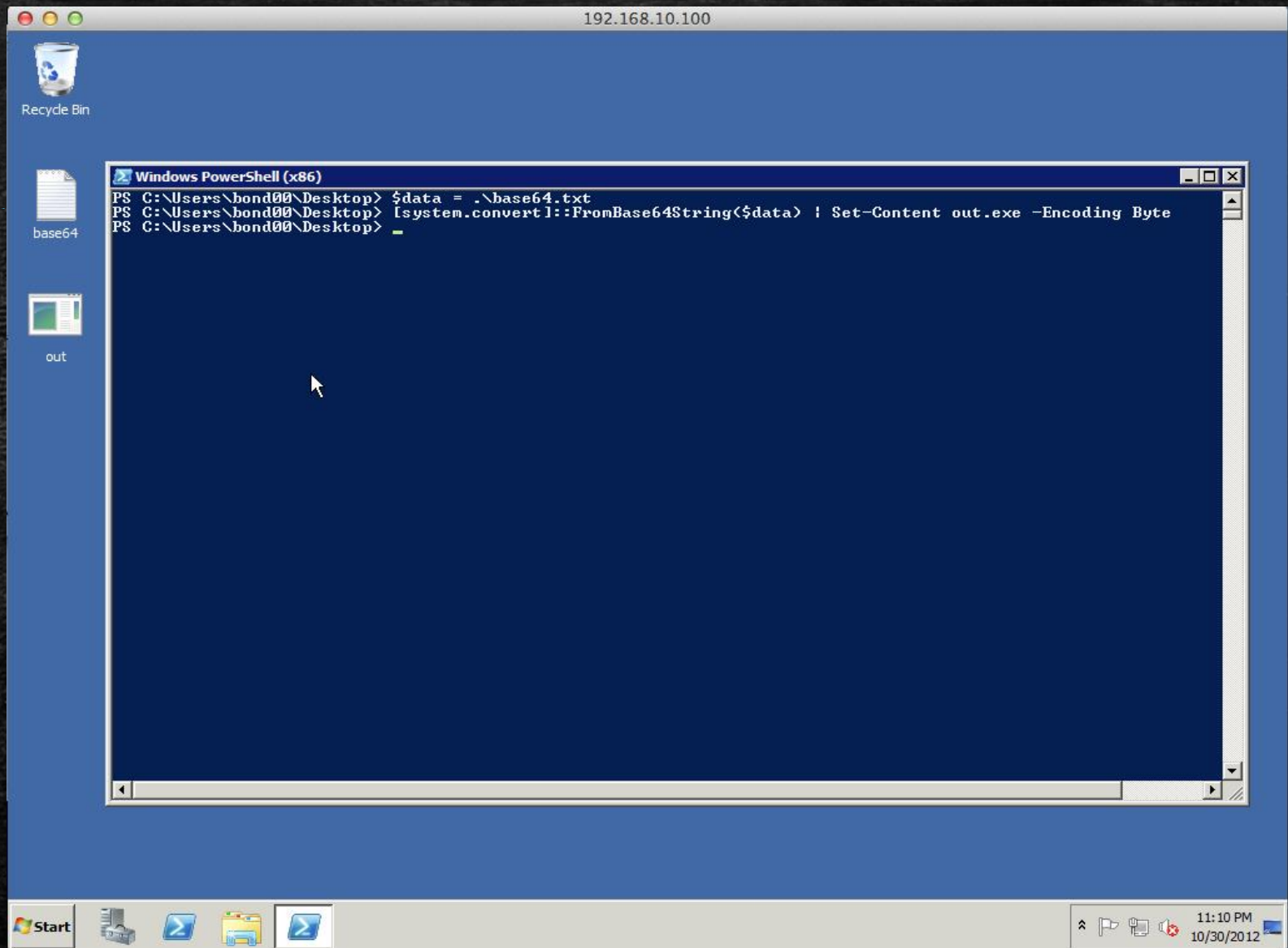
## Countermeasures

- Block outbound all, lock down proxy, block outbound SYN in DMZ









192.168.10.100



```
Windows PowerShell (x86)
PS C:\Users\bond00\Desktop> $data = .\base64.txt
PS C:\Users\bond00\Desktop> [system.convert]::FromBase64String($data) | Set-Content out.exe -Encoding Byte
PS C:\Users\bond00\Desktop> _
```



# TTPs

---

## Persistence APT style

- Nothing good out there...
  - Meterpreter – OSS
  - Core Impact – \$\$\$\$
  - Poison Ivy – Private
  - DarkComet – Private
- Who's going to trust these?

## Techniques

- DLL hijacking
- Service
- Applnit registry
- DLL wrapper



dribbleglass.com

# PERSISTENCE

Think of that restraining order  
as a "suggestion."



# TTPs

Go custom or go home...



Action	Command	Arguments	RunAs
Select one ..			
Select one ..			
GetProcess List			
GetDirectory Listing			
Check Network Connections			
Run a Command			
Check Installed Software			
Delete File			
Execute a file			
Sleep			
Download & Execute Exe			
Download File			
Download & Execute DLL			
Download & Execute Shellcode			

# TTPs

## DATA EXFILTRATION METHODOLOGY

### Step One: C2 Communication

The malware contacts C2 servers for instructions, such as downloading and executing new malware or opening a reverse backdoor — allowing the attacker full access to the compromised system, bypassing firewall restrictions.

### Step Two: Attack

The attacker (through the reverse backdoor) compromises multiple sources of interest, such as database servers, email servers, and file share servers.

### Step Three: Data Staging

The attacker sends data to a staging server. Once the data is set, the attacker then compresses the data (using the rar.exe utility) and password protects it.

### Step Four: Data Exfiltration

The attacker uses malware to send the data through an encrypted tunnel to a malicious external IP address.





# Conclusion

---

# Conclusion

---

## Know your network

- That means monitor the traffic  
Netflow, signatures, baselines

## Egress Filtering

- Like it is going out of style

## Proxy or die!

- Proxy all traffic
- Break & Proxy HTTPS traffic
- Look out for base64 encoding
- If you can't inspect it...  
You just made someone's b-day ☺



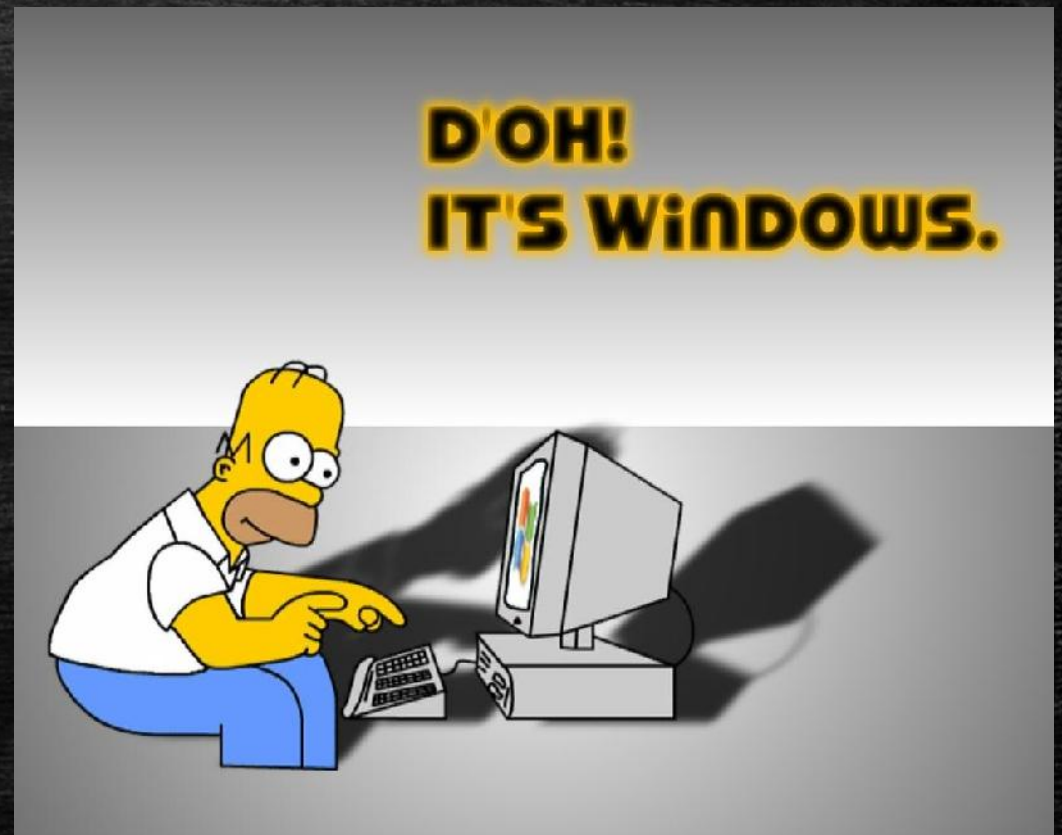


# Conclusion

---

It's not the appliance / server /  
IDS / IPS / software / device's  
fault...

Expecting your network  
devices to identify unknown  
traffic is like expecting your  
AV to detect a 0-day.



# Conclusion

---

Testing should be modeled after threats

- Vulnerability scans don't cut it
- Correct practice makes perfect



IF YOU ENGAGE IN  
**RISKY BEHAVIOR**



YOU SHOULD GET TESTED ONCE A YEAR



# Conclusion

---

Offense is sexy, defense is lame

- We need to change the way we think about the problems.



# Conclusion

---

The attackers have them, do you?





# The End!

---

Questions?

## Contact Information

- Brady Bloxham
- Silent Break Security
- [brady@silentbreaksecurity.com](mailto:brady@silentbreaksecurity.com)
- [www.silentbreaksecurity.com](http://www.silentbreaksecurity.com)
- (801) 855-6599