



The Disappearing Patch Window

Observations from the Internet Storm Center

Johannes B. Ullrich, Ph.D.

SANS Institute

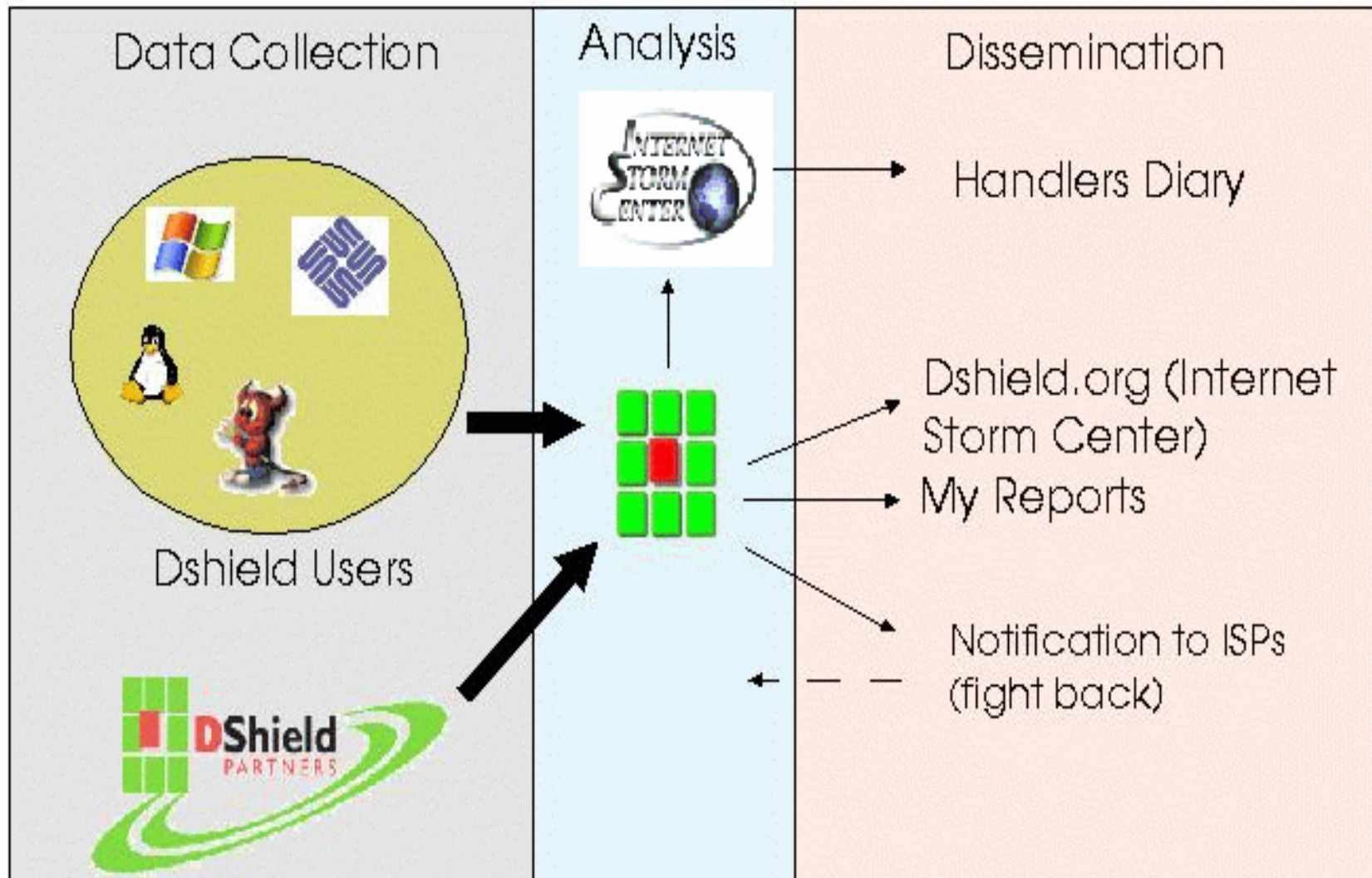
jullrich@sans.org

Outline

- Introduction to the ISC
 - Distributed Sensors and DShield.org
 - Data Analysis and the Handlers List
- Patch Window Observations: MS04-011
 - MS04-011: LSASS and SSL-PCT Vulnerabilities
 - PoC Exploits
 - “Bots”
 - The Sasser Worm
 - Download.ject/BerBew/Scob
- Conclusion, Q&A



The Internet Storm Center





Participating

- Submit Firewall Logs
 - Large number of firewalls supported. For an up to date list see <http://www.dshield.org/howto.php>
 - Reports can be submitted anonymously. No network is too small!
- Report incidents to the handlers team.
 - Odd binaries found, exploit sightings, tips to prevent incidents or educate users.

Using the ISC



SANS SANS Homepage SANS Bookstore SANS Reading Room SANS Portal

Infocon: **GREEN**  **FEATURING THE: INTERNET STORM CENTER** [Register Now!](#)

Handler on Duty: **Jim Clausing** 02:49:38 UTC Jun 28 2004 22:49:38 Jun 27 2004

Trends Top 10 Reports Contact About INFOCon Links XML

Handler's Diary: Continued Sighting of Download.Ject; WiFi Security

Port Lookup: 8000 [graph](#) [details](#)

[search](#)

+ Port Graph

- Port History

- Today's Diary

+ Papers and Analysis

+ Survival Time

Interested in participating? Click here to find out how to do so.

Today's Diary

Previous

Handlers Diary June 27th 2004

Updated June 27th 2004 23:21 UTC (Handler: Tony Carothers)

Continued Sighting of Download.Ject; WiFi Security

Continued Sighting of Download.Ject

While the majority of the traffic has died down, we are still receiving reports of administrators finding log files with indicators of msits.exe download. We would like to remind all users that even though the main issue is over, the same exploit is continuing to be used by web sites out there for malicious purposes. Practically all of the major antivirus services have signatures for this exploit, which is also known as JS.Scob.Trojan, Scob, and JS.Toofeer.

Port History



Category	Value
Red Dashed	135
Blue Solid	445
Black Dashed	17300
Green Solid	80
Green Dashed	2745

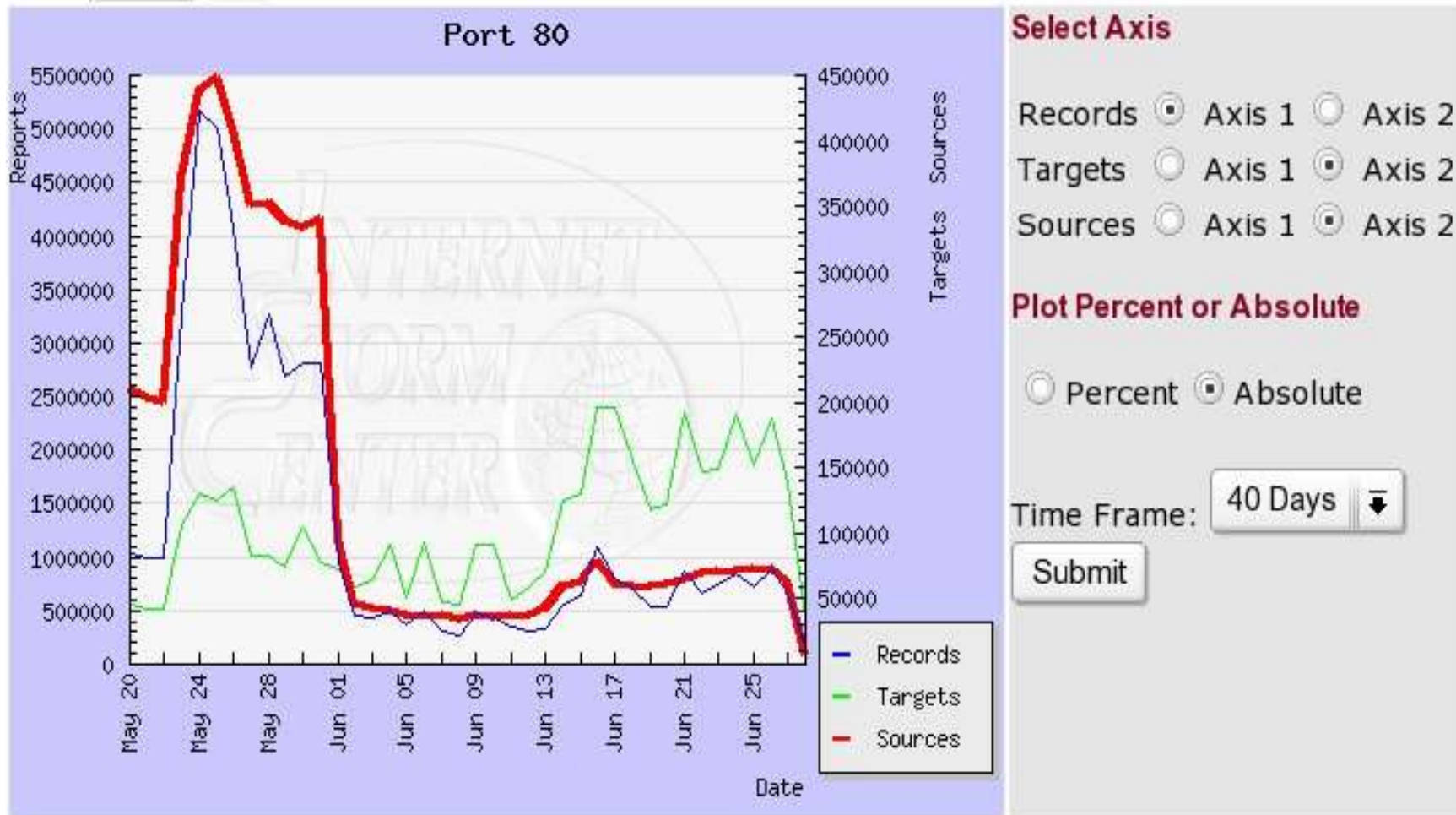
Diary Archive

27-Jun - Continued Sighting of Download.Ject; WiFi Security

26-Jun - Download.Ject Detection and Recovery -- New Phishing Attack Technique

Port Details (Part 1)

Port:



Port Details (Part 2)

Raw Data

Date	Sources	Targets	Records
2004-06-28	6615	33926	167903
2004-06-27	63062	138607	659172
2004-06-26	72158	187061	896403
2004-06-25	72794	151413	724609
2004-06-24	70988	191925	846923
2004-06-23	70462	148029	749088

Services registered for this port (from Neohapsis)

Protocol	Service	Name
tcp	www	World Wide Web HTTP
udp	www	World Wide Web HTTP
tcp	711trojan	[trojan] 711 trojan (Seven Eleven)

Vulnerabilities for this port (from CVE)

CVE ID	Protocol	Source Port	Targetport
Description			
CVE-2001-0987	tcp	any	80
Cross-site scripting vulnerability in CGIWrap before 3.7 allows remote attackers to execute arbitrary Javascript on other web clients by causing the Javascript to be inserted into error messages that are generated by CGIWrap.			
CVE-2001-0805	tcp	any	80
Directory traversal vulnerability in ttawebtop.cgi in Tarantella Enterprise 3.00 and 3.01 allows			

User Comments

Got any comments regarding this port? Click [here](#) to share.

Port 4672/udp is used by the emule file sharing software.

http://www.emule-project.net/home/perl/help.cgi?l=2&topic_id=27&r

full comment

Submitted by: arzie (Jun 20th 2004)

Handlers List

- 30 diverse security professionals
 - geographic (Europe, Asia, North-Am., South-Am.)
 - background (ISP, financial, government, education)
- Each day, a particular handler is designated 'handler of the day'
- To submit reports to the handler list, use the 'contact' form (<http://isc.sans.org/contact.php>)



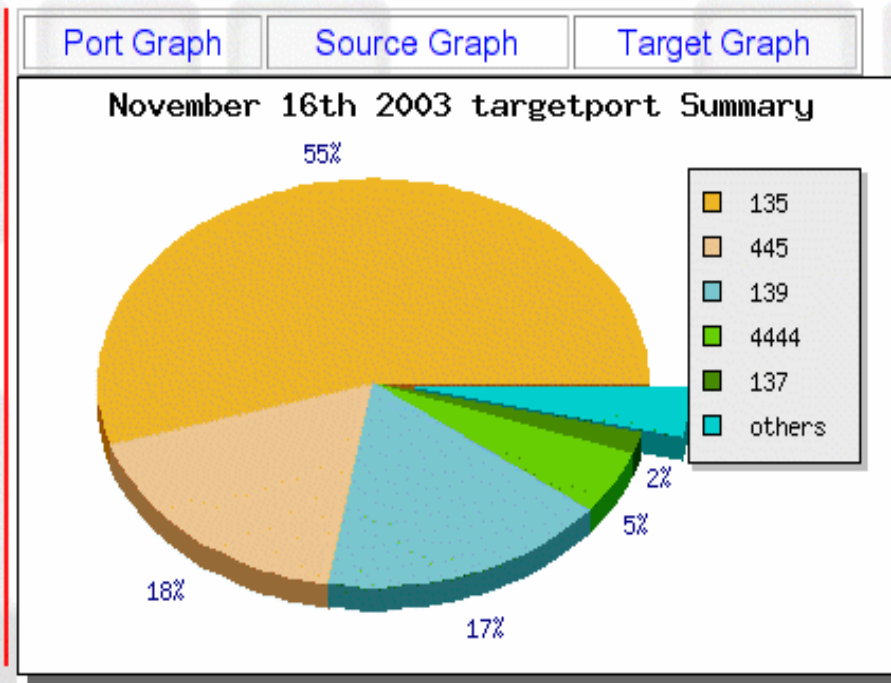
DShield Submitter Features (1)

ed on 2003-11-16:

els': high medium low misconf.

rk Severity based on Target Port):

low Possible Firewall Misconfiguration



Date	Time	Source	Source Port	Target	Target Port	Protocol	Danger
2003-11-16	02:16:54	213.115.058.092	500	010.000.000.049	500	17	●
2003-11-16	02:16:54	213.115.058.092	500	010.000.000.050	500	17	●
2003-11-16	02:17:28	217.031.160.002	43184	010.000.000.050	53182	6	○
2003-11-16	02:20:51	068.166.250.094	1637	010.166.125.210	135	6	●
2003-11-16	02:20:51	068.166.250.094	1638	010.166.125.211	135	6	●



DShield Submitter Features (2)

Date: Nov-16-2003

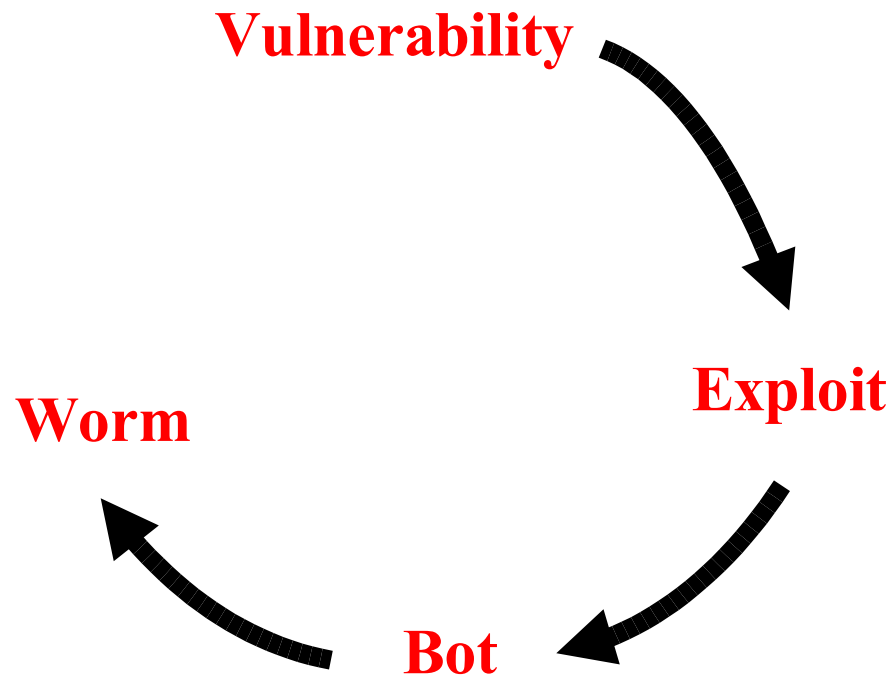
Lines: 31971

Limit: 320 (lines and columns with less hits are not shown)

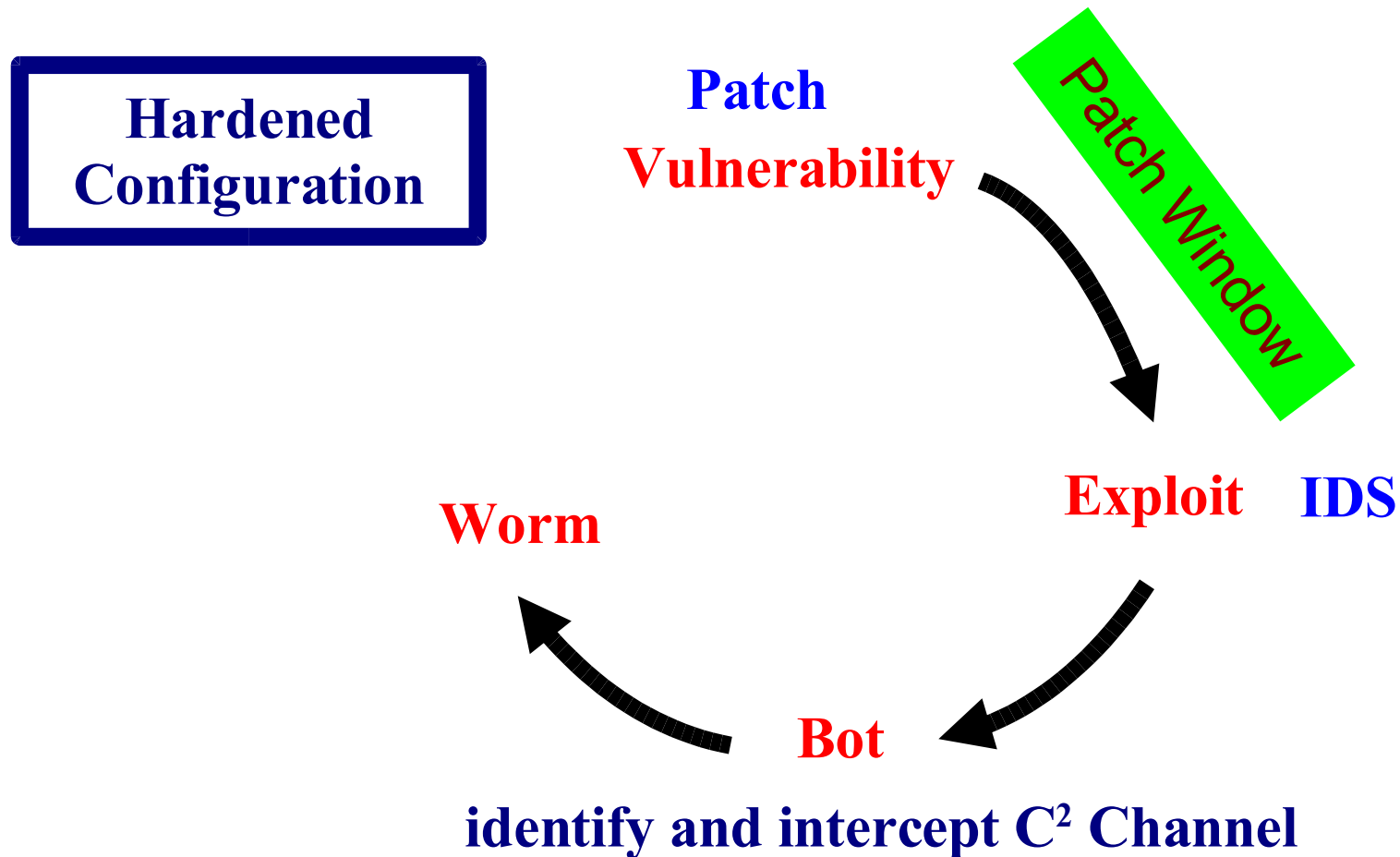
Submit

731900	source	207.201.229.042	061.161.082.179	068.156.168.098	211.023.110.194	061.177.075.214
targetport	totals	6504	914	816	534	532
135	17559	10				
445	5610	3257	308	414	273	240
139	5396	3237	576	402	261	229
4444	1610					
137	552		30			63

Malware Life Cycle



Malware Life Cycle / Patch Window



Malware Life Cycle-Stage 1: Vulnerability



- Example: MS04-011

- LSASS

- Default Configuration Vulnerable
 - Allows full system access
 - “Simple” overflow

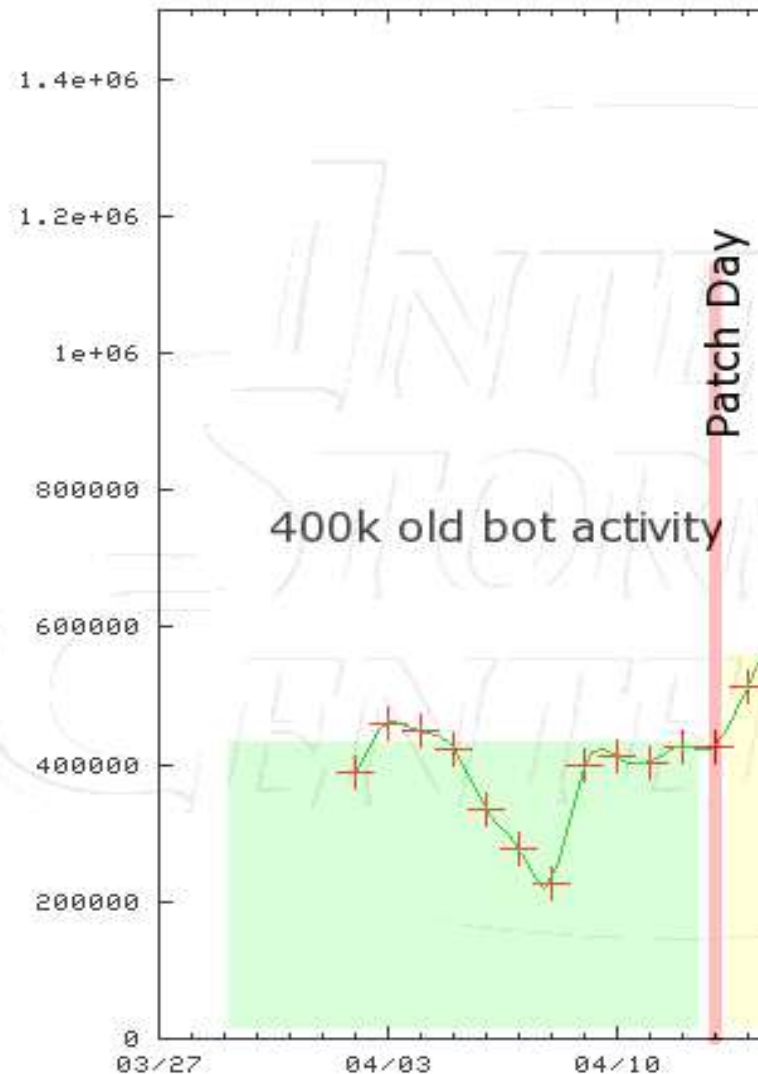
- SSL-PCT

- IIS and SSL has to be enabled. While IIS is enabled by default, SSL is not enabled by default and it is not easy to enable.
 - Allows full system access
 - “Simple” overflow

A calendar for the month of April 2004. The calendar is displayed on a cyan background. The word "April" is written in a large, black, serif font at the top center. The days of the month are arranged in a grid. The 1st, 2nd, and 3rd are in the first row. The 4th through 10th are in the second row. The 11th through 17th are in the third row. The 18th through 24th are in the fourth row. The 25th through 30th are in the fifth row. The 13th is highlighted in blue. The 3rd, 10th, 17th, 24th, and 25th are highlighted in red.

April							1	2	3
4	5	6	7	8	9	10			
11	12	13	14	15	16	17			
18	19	20	21	22	23	24			
25	26	27	28	29	30				

ISC Data – Port 445 after “Patch Day”

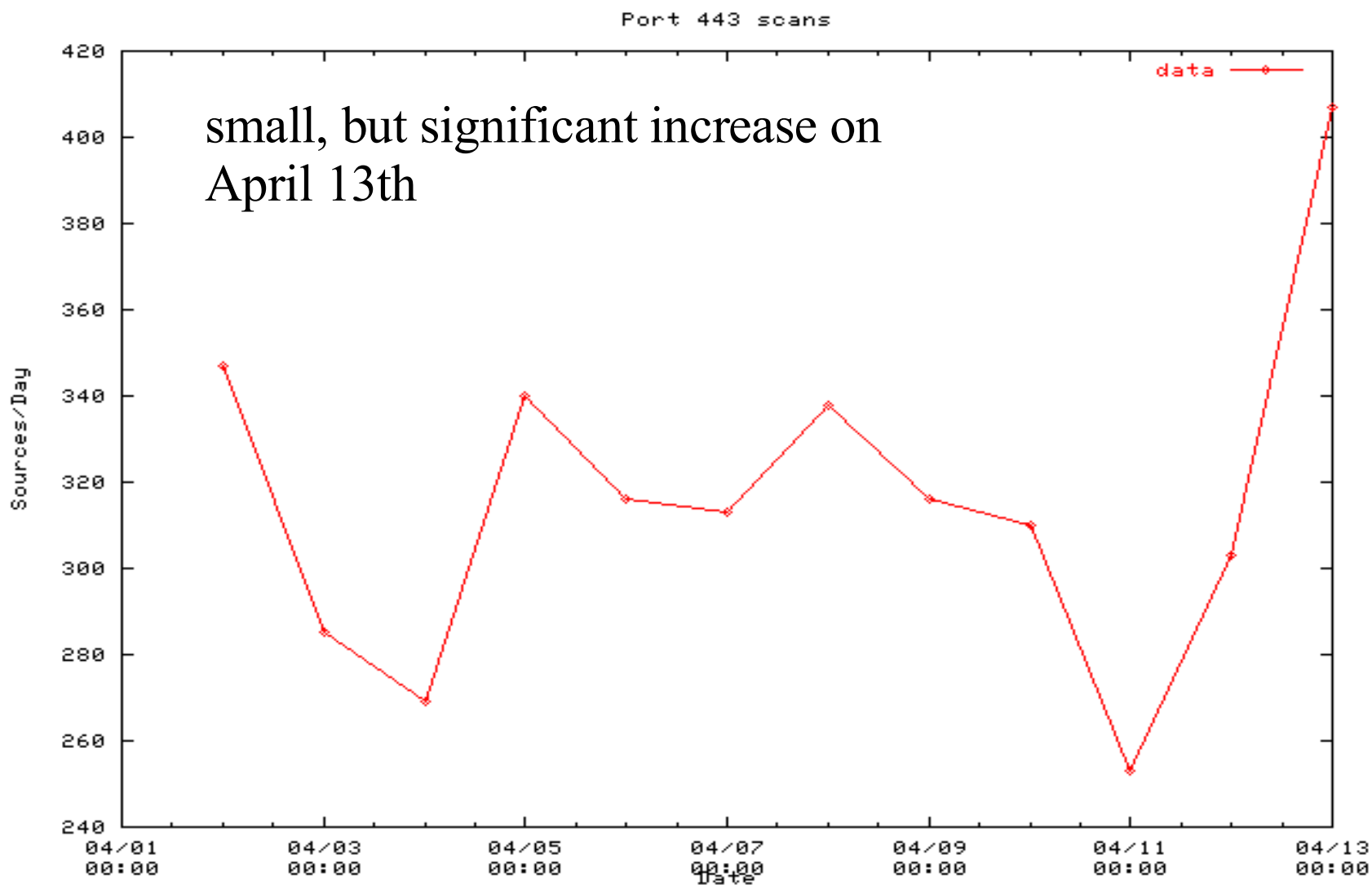


Graph shows number of source IPs scanning port 445 tcp.

- Immediate jump (target list acquisition)
- High background (port used for other exploits, e.g. simple password brute forcing)

FIXED

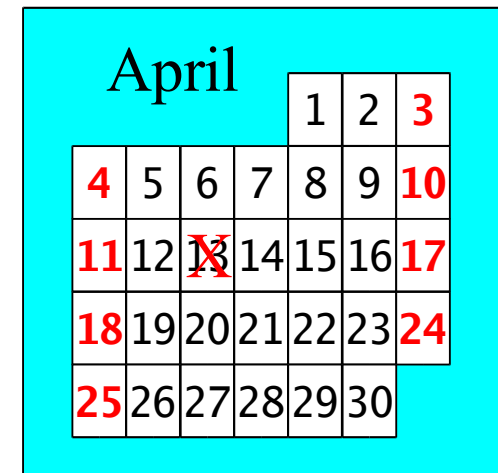
ISC Data: Port 443 post patch day



Countermeasures: Hardening

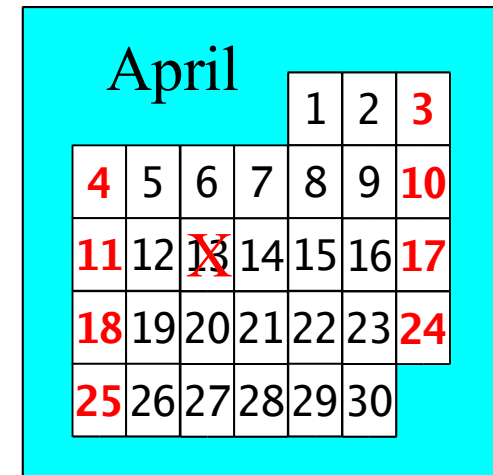
- A hardened system configuration will provide an important head start to the defender and will put the initiative back to the defending team.
- For LSASS:
 - Close port 445.
 - Limited access to VPN/LAN.
- For SSL-PCT:
 - Limit IIS access to system.
 - Harden IIS according to CIS gold standard.

(<http://www.cisecurity.org>)

A calendar for the month of April. The days of the month are arranged in a grid. The numbers 3, 10, 17, 24, and 25 are highlighted in red. The number 13 is crossed out with a red 'X'.

Countermeasure: Patch

- The most promising countermeasure against a Vulnerability is a patch.
- Reactive. You can not patch against unknown vulnerabilities.
- Time consuming. Patches have to be validated and may interfere with other software.
- In this particular case, the patch as released in MS04-011 fixed a large number of problems, and causing issues in some instances (e.g. Novell VPN Client, KB Article 835732)

A calendar grid for the month of April. The days of the month are arranged in a grid. The numbers 3, 10, 17, 24, and 25 are highlighted in red. The number 13 is crossed out with a red 'X'.

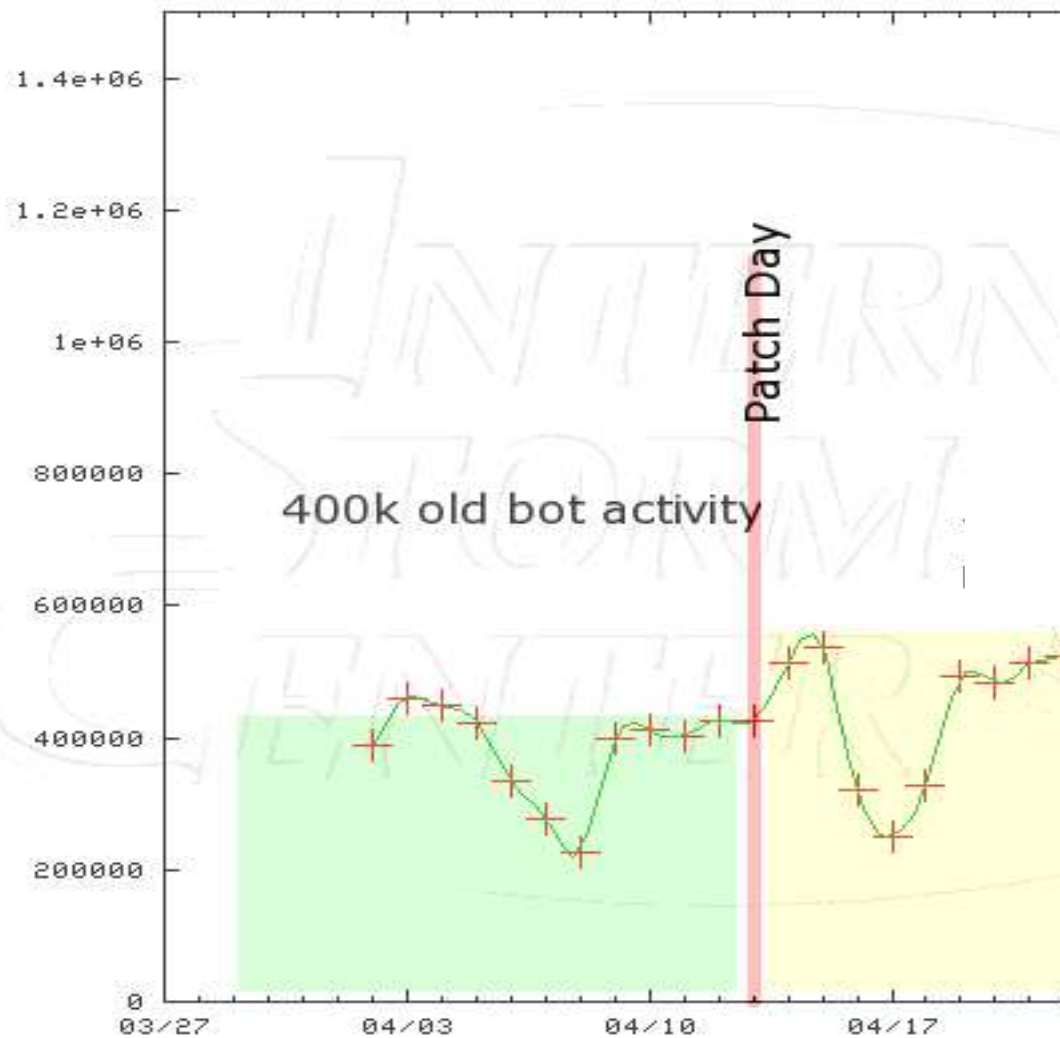
Malware Life Cycle-Stage 2: Exploit

- Patch Available: April 13 (MS04-011)
- First mention of an exploit for LSASS & SSL: April 14 (Dave Aitel, Full Disclosure)
- Exploit available to public: April 21 (K-Otic, Full Disclosure)
- Exploit seen used in the wild same day, widespread use around April 23rd.

April						
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	



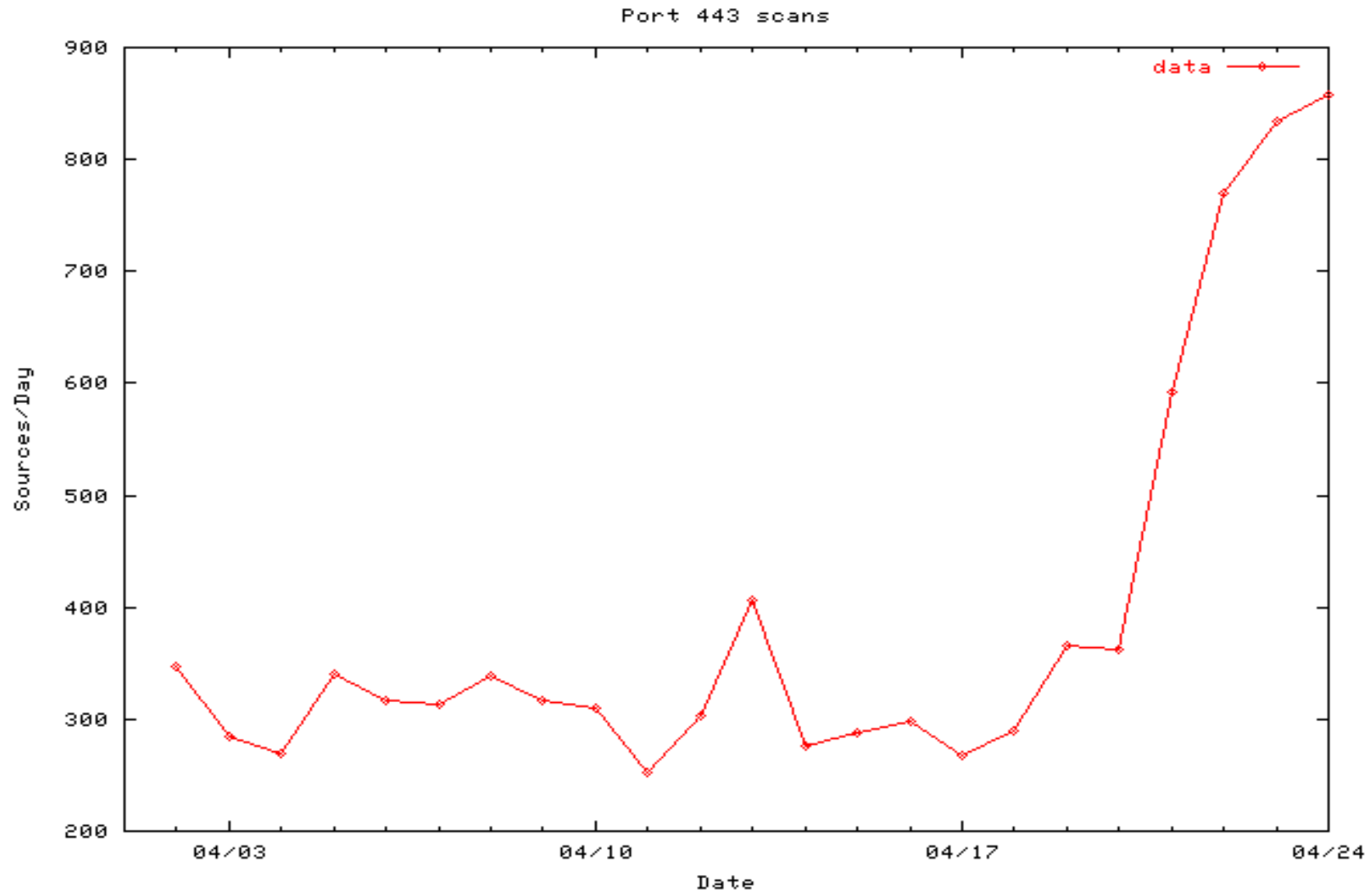
Port 445 – Exploit Phase



drop after patch day (weekend)

increase soon after as exploits arrive.

ISC Data: Port 443 (exploit phase)





Countermeasure: IDS

- **Hardened Configuration: CIS Gold Standard**
 - Patch Available: April 13 (MS04-011)
- **Patch Systems, review Configuration. (ISC diary April 13th)**
 - First mention of an exploit for LSASS & SSL: April 14 (Full Disclosure, Dave Aitel)
- **Snort signatures (ISC Diary April 15th)**
 - Exploit available to public: April 21 (Full Disclosure, K-Otic)
 - Exploit seen used in the wild same day, widespread use around April 23rd .

Malware Life Cycle-Stage 3: Bot

- LSASS exploit incorporated into Phatbot/Agobot.
- Targeted initially at University Networks, later at high speed consumer networks (DSL/Cable).
- Bots allow for power full remote control for various purposes (DDOS, spam relay, anonymous proxy)
- Hard to detect by antivirus software. Bots are ephemeral and built from components to match a target's vulnerabilities.

April

						1	2	3
4	5	6	7	8	9	10		
11	12	13	14	15	16	17		
18	19	20	21	22	23	24		
25	26	27	28	29	30			



Countermeasure: Disrupting Bots

Methods

- Identify binaries and submit to AV vendors.
- Identify C&C channels.

April

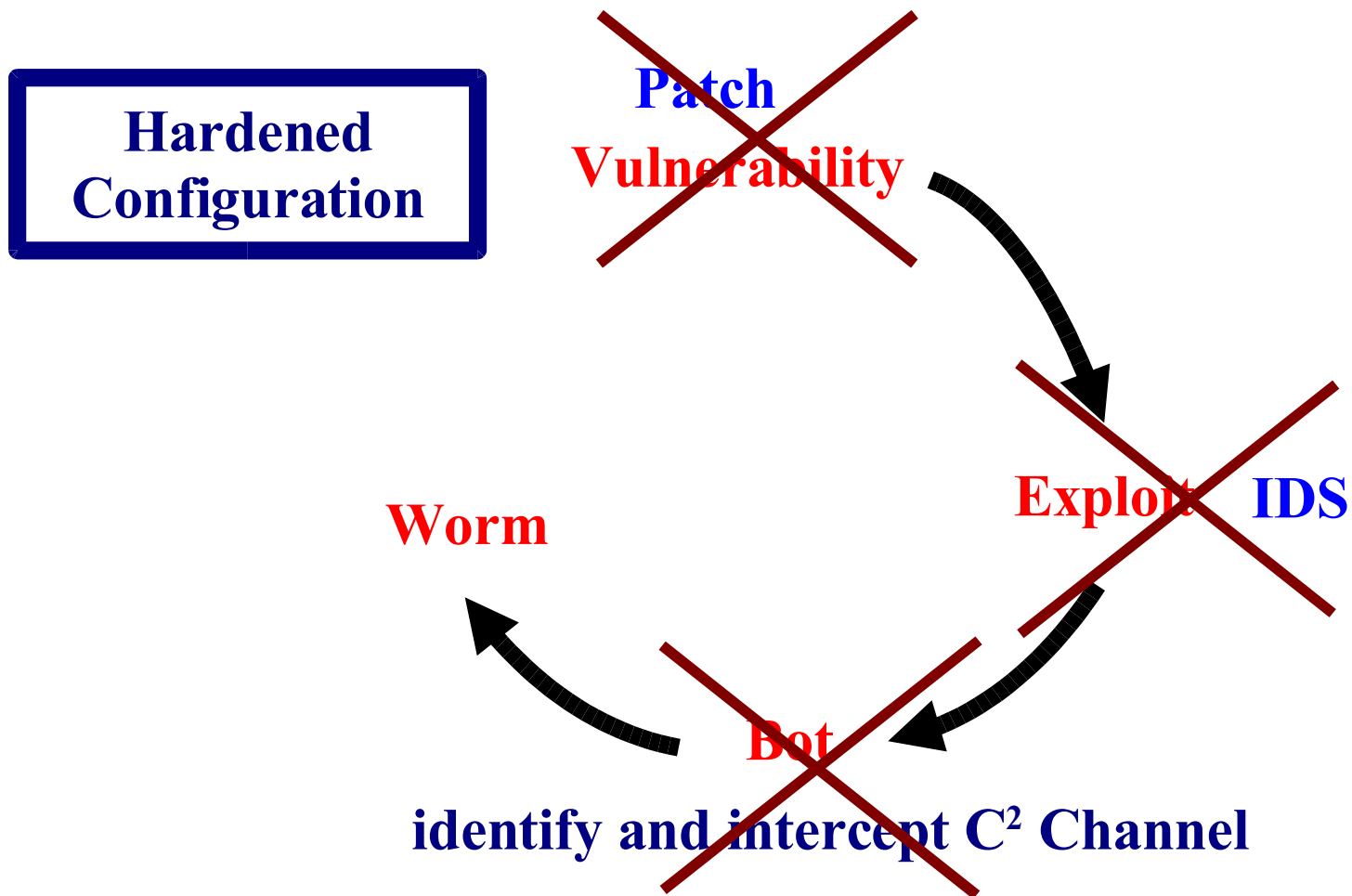
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

Problems

- Reactive
- Slow (24-48 hrs)
- “Whack The Mole”



Review: Malware Lifecycle



Sasser Worm

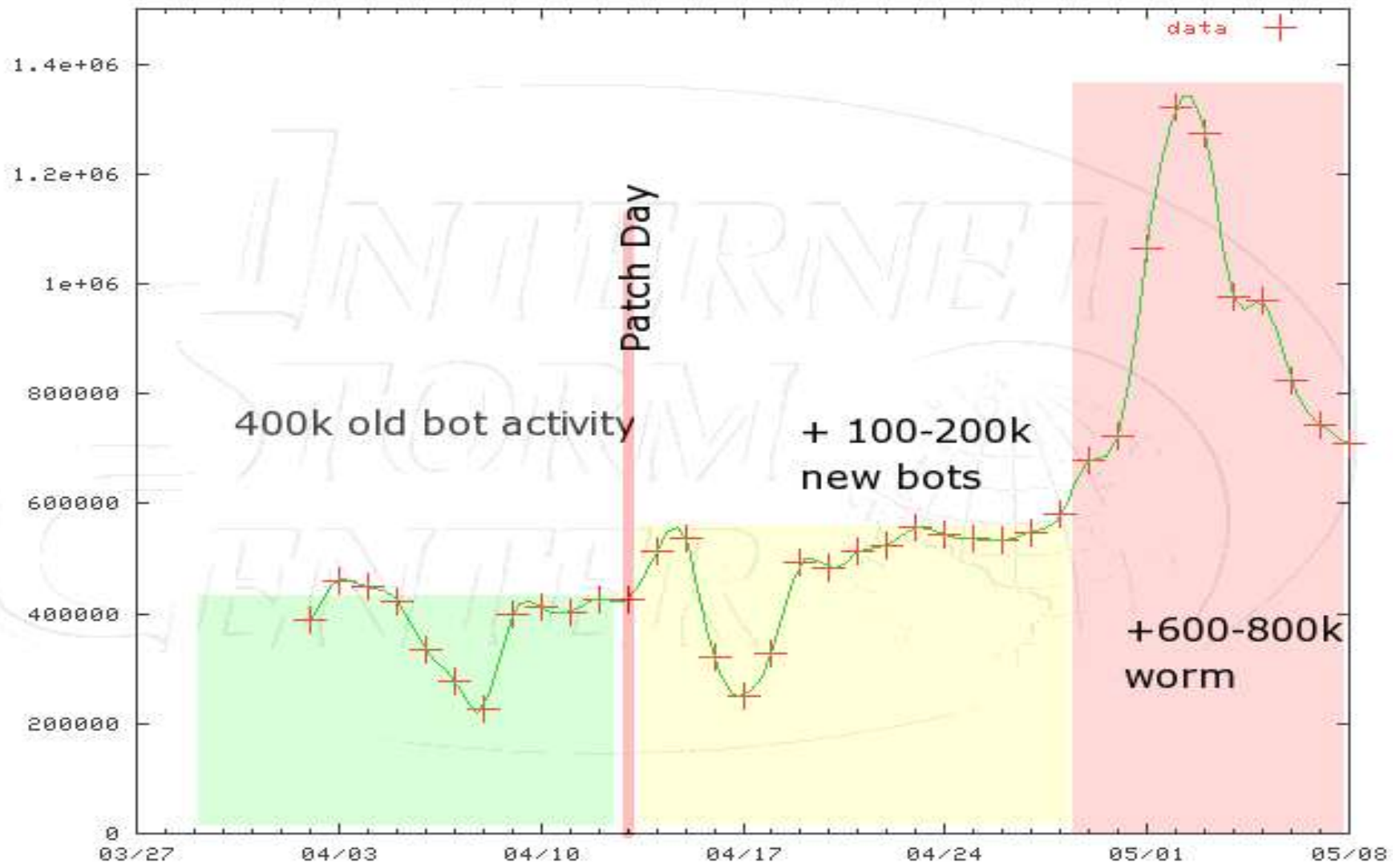
- Graffiti worm.
- Installs simple ftp server to spread itself.
- Impact similar to 'Blaster'.
- Tcp worm requiring full connect with initially few threads: slow spread over a couple days.
- Based on MSFT patch download, 1.6 Million victims.

April

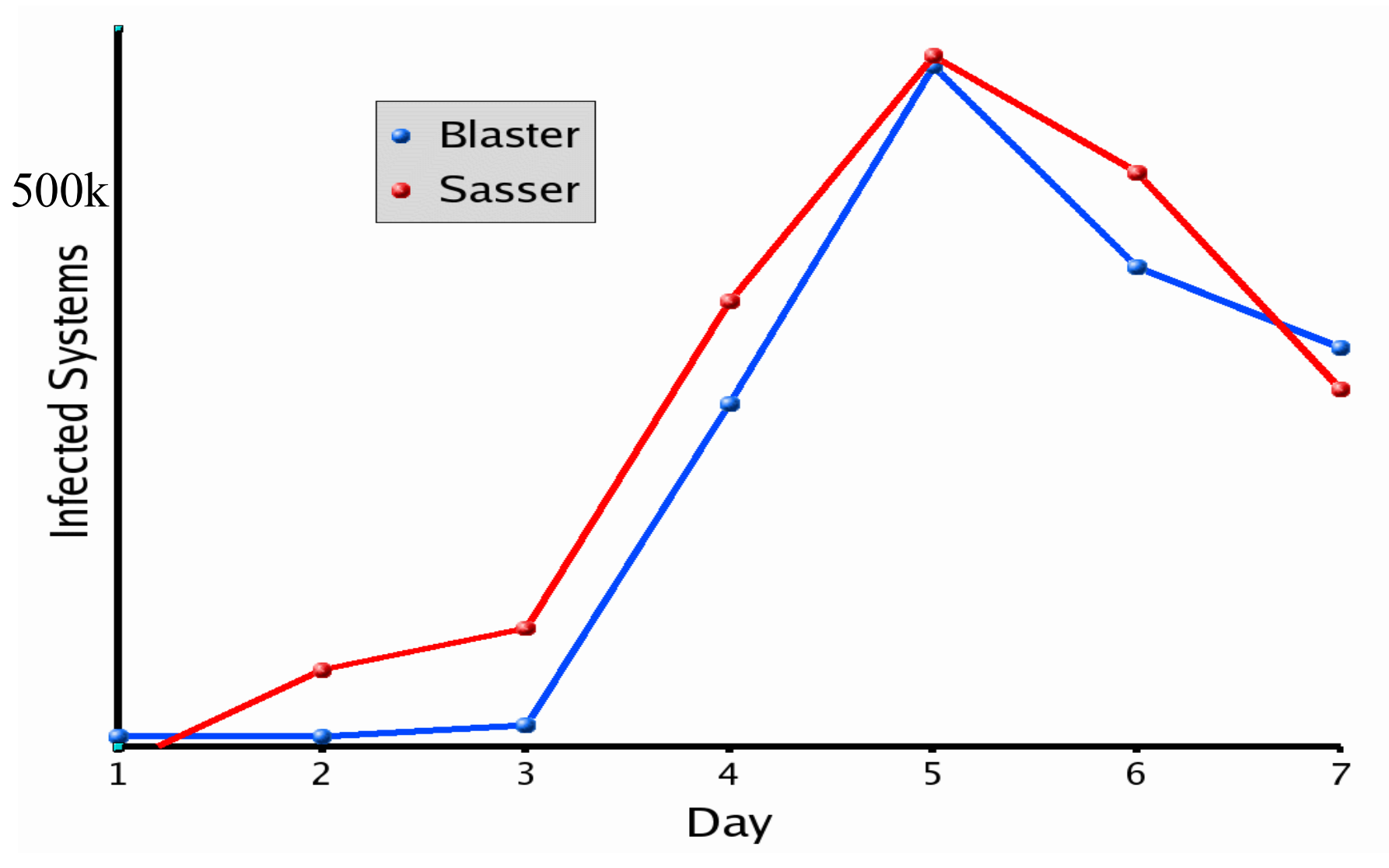
					1	2	3
4	5	6	7	8	9	10	
11	12	13	14	15	16	17	
18	19	20	21	22	23	24	
25	26	27	28	29	30		



Port 445: ISC Data



Compare Sasser & Blaster



What about SSL-PCT?

LSASS

- Vulnerability applies to default configuration.
- Many vulnerable systems are home/unmanaged systems.
- Systems typically of lower value.

SSL-PCT

- Not vulnerable in default configuration.
- Less home/unmanaged systems.
- Higher value systems.

RESULT: SSL-PCT worm would have little impact and destroy valuable resources.

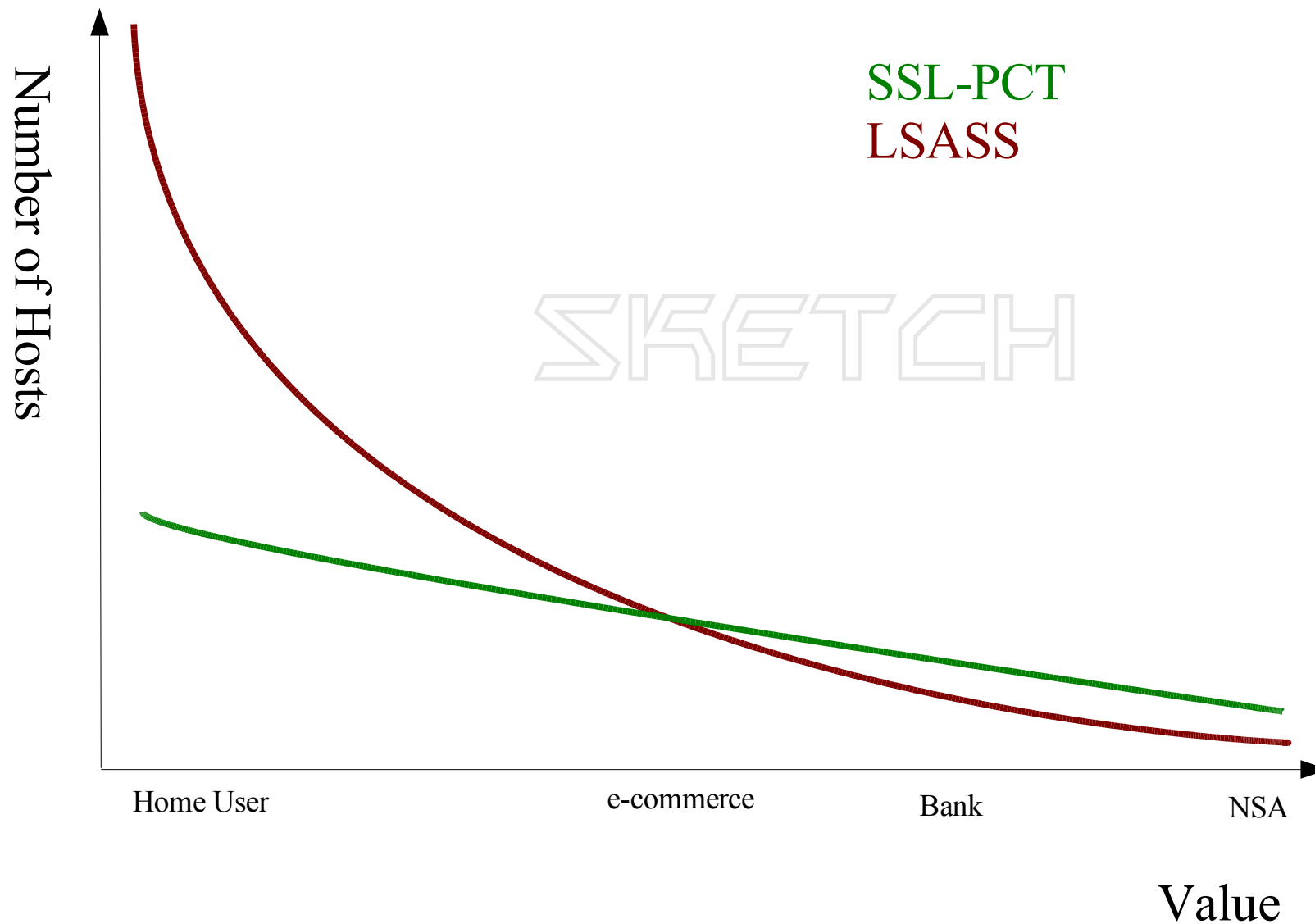


SSL-PCT Aftermath

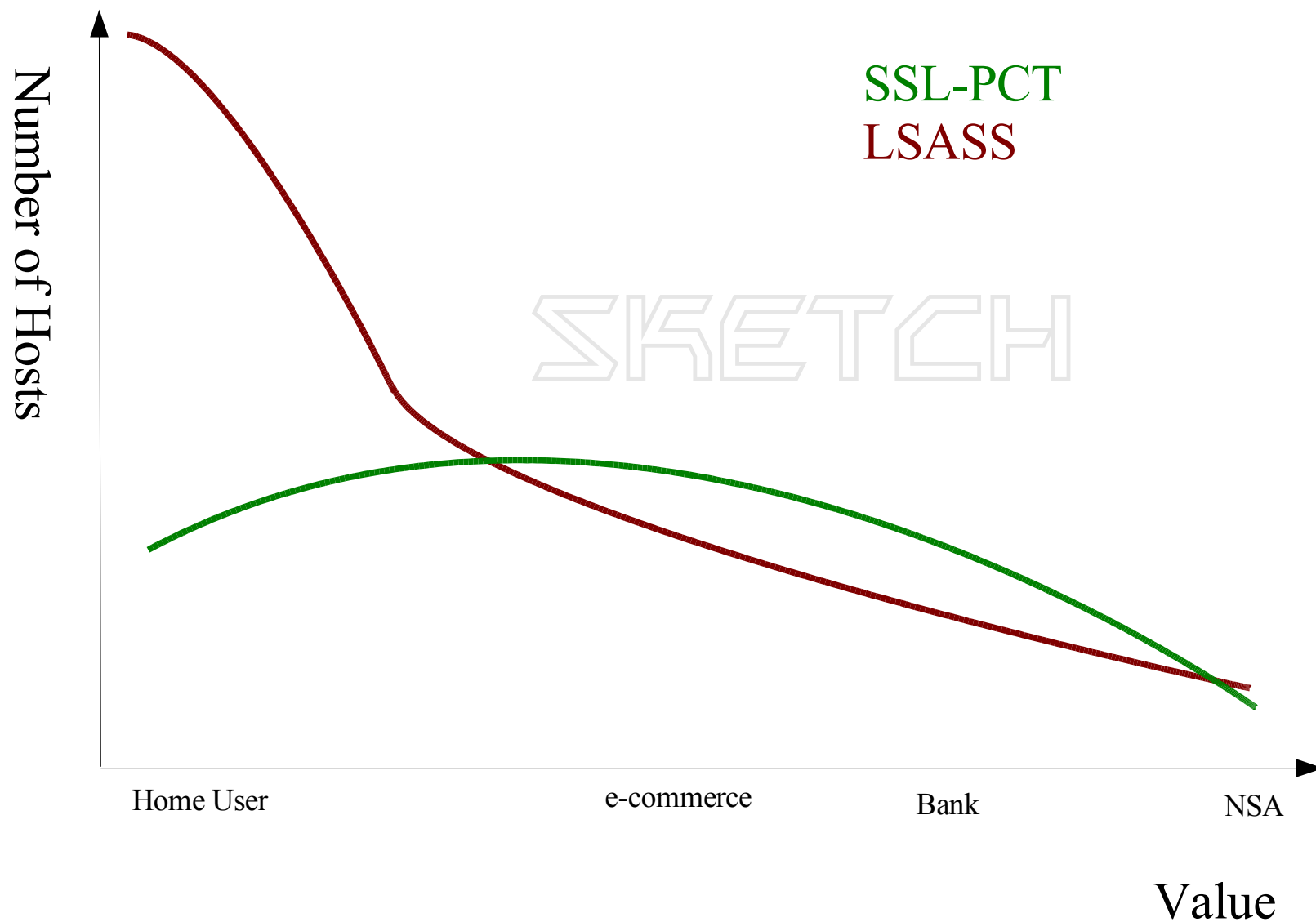
- Russian HangUp group collects number of hosts, likely using the SSL-PCT exploit.
- Installs 'Download.ject' script using an UNPATCHED Microsoft Internet Explorer Exploit
- Uses Download.ject to install 'Brebar' on systems visiting “defaced” sites.
- Initially, virus scanners did not catch any component (only Symantec warned users upon visiting the sites)

USE OF HIGH VALUE TARGETS FOR HIGH VALUE ATTACK.

Host Value



Cumulative Host Value



Download.ject/BerBew/Scob

- Scans show 600+ exploited web sites.
- Likely 1,000-10,000 victims.
- We are not aware of any exploited web site notifying its customers (hard to do in some cases).
- Trojan attempted to steal bank passwords.
- Same HangUp crew linked to a number of additional viruses/bots with financial motives. Based in Russia.



Conclusion

- Only defence is hardened configuration.
- Exploits happen shortly after a vulnerability is released.
- Saturation is achieved very quickly after a public exploit is released.
- Even vulnerabilities not suitable for a 'worm' are frequently used on a larger scale with devastating effect.
- Worms are indicators of saturation, not indicators to start patching.

Conclusion



Please participate:

- Send logs to DShield

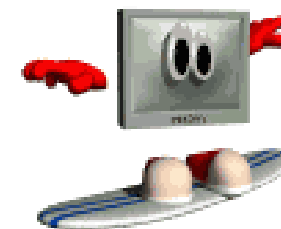
(<http://www.dshield.org/howto.php>)

- Submit observations to the ISC

(<http://isc.sans.org/contact.php> , handlers@sans.org)

- Learn how to harden your system

(<http://www.sans.org>)



jullrich@sans.org

END



END