# Botnets and Cybercrime

Corso di Sicurezza delle reti e dei sistemi software aa 2016/17

Ing. Antonio Pirozzi

### Some definitions

- "A botnet is a collection of computers, connected to the internet, that interact to accomplish some distributed task." 1
- Controlled by one person or a group of people (aka. the botmaster) under a command and control structure (C&C)
- The word botnet is a combination of the words <u>robot</u> and <u>network</u>.



### Botnet components

- C&C : The C&C manages a list of infected machines; it monitors their status and gives them operative instructions.
- **BOT**: A "bot" is a type of malware that allows an attacker to take control over an affected computer. Also known as "Web robots", bots are usually part of a network of infected machines, known as a botnet 2
- **Zombie**: victim machines



Police have arrested Algerian national Hamza Bendelladj, who is wanted by the FBI for cyber crimes. (Photo by Somchai Poomlard)

### Botmaster

known as **Bx1** is an Algerian computer hacker. Using log-in information obtained from a <u>Trojan horse</u> called <u>SpyEye</u> was sentenced to 15 years in prison



On May 9, 2006, Jeanson James Ancheta became the first person to be charged for controlling large numbers of hijacked computers or <u>botnets</u>

### motivations

Cybercriminals cause harm with botnets in many ways:

Sending	Stealing	<b>DoS</b> (Denial of Service)	Clickfraud
They send - spam - viruses - spyware	They steal personal and private information and communicate it back to the malicious user: - credit card numbers - bank credentials - other sensitive personal information	Launching denial of service (DoS) attacks against a specified target. Cybercriminals extort money from Web site owners, in exchange for regaining control of the compromised sites. More commonly, however, the systems of everyday users are the targets of these attacks for the simple thrill of the botherder.	Fraudsters use bots to boost Web advertising billings by automatically clicking on Internet ads.

Additionally, botnets can also be used to mine bitcoins, intercept any data in transit, send logs that contain sensitive user information

3 https://us.norton.com/botn

### Architecture evolution

- Botnet Architecture evolved over time
- Advanced topology is more resilient to shutdown, enumeration or discovery
- No need for C&C? relying on a C&C server is a limitation
- IRC botnets were especially prevalent in the 1990s and early to mid 2000's. Such botnets basically are comprised of a collection of infected systems that are controlled remotely via a preconfigured IRC server and channel.

### Architecture evolution

#### • More UDP, less TCP

- The bots would contact each other by using a sort of homemade UDP handshake. If successful, this would cause the bots to exchange TCP data, such as configuration files, list of other peers, etc
- TCP communications are easy to track and dump, and the bot does not perform any authentication on the packets exchanged, so anyone can impersonate a bot and successfully communicate with other bots, downloading stuff like configuration data.

Source	Destination	Protocol	Info	
	24.99.214.31	UDP	Source port: 2	28118 Destination port: 17431
24.99.214.31		UDP	Source port: 1	17431 Destination port: 28118
	24.99.214.31	UDP	Source port: 2	28118 Destination port: 17431
24.99.214.31		UDP	Source port: 1	17431 Destination port: 28118
	24.99.214.31	TCP	xrl > 26678 [s	SYN] Seq=0 Win=64240 Len=0 MSS=1
24.99.214.31		TCP	26678 > xrl [s	SYN, ACK] Seq=0 Ack=1 Win=8192 (
	24.99.214.31	TCP	xrl > 26678 [A	ACK] Seq=1 Ack=1 Win=64240 Len=0
	24.99.214.31	TCP	xrl > 26678 [F	PSH, ACK] Seq=1 Ack=1 Win=64240
24.99.214.31		TCP	26678 > xrl [F	РSH, АСК] Seq=1 Ack=45 Win=64240
24.99.214.31		TCP	26678 > xrl [A	ACK] Seq=5 Ack=45 win=64240 Len=
	24.99.214.31	TCP	xrl > 26678 [A	АСК] Seq=45 Ack=1465 Win=64240 Ц
24.99.214.31		TCP	26678 > xrl [A	АСК] Seq=1465 Ack=45 Win=64240 Ц
24.99.214.31		TCP	26678 > xrl [A	АСК] seq=2925 Ack=45 win=64240 (
	24.99.214.31	TCP	xrl > 26678 [A	АСК] Seq=45 Ack=4385 Win=64240 Ц
24.99.214.31		TCP	26678 > xrl [A	ACK] Seq=4385 Ack=45 Win=64240 L

https://www.symantec.com/connect/blogs/zeusbotspyeye-p2p-updated-fortifying-botne75.1

Source	Destination	Protocol	Info					
	68.173.14.233	UDP	Source	port:	10197	Destination	port:	29211
68.173.14.233		UDP	Sounce	port:	29211	Destination	port:	10197
	68.173.14.233	UDP	Source	port:	10197	Destination	port:	29211
68.173.14.233		UDP	Sounce	port:	29211	Destination	port:	10197
68.173.14.233		UDP	Source	port:	29211	Destination	port:	10197
68.173.14.233		UDP	Sounce	port:	29211	Destination	port:	10197
68.173.14.233		UDP	Sounce	port:	29211	Destination	port:	10197
68.173.14.233		UDP	Sounce	port:	29211	Destination	port:	10197
	75.15.147.68	UDP	Sounce	port:	10197	Destination	port:	27208
	68.173.14.233	UDP	Sounce	port:	10197	Destination	port:	29211
68.173.14.233		UDP	Sounce	port:	29211	Destination	port:	10197
	68.173.14.233	UDP	Sounce	port:	10197	Destination	port:	29211
68.173.14.233		UDP	Source	port:	29211	Destination	port:	10197
75.15.147.68		UDP	Sounce	port:	27208	Destination	port:	10197
	68.173.14.233	UDP	Sounce	port:	10197	Destination	port:	29211
	75.15.147.68	UDP	Sounce	port:	10197	Destination	port:	27208
68.173.14.233		UDP	Sounce	port:	29211	Destination	port:	10197
	68.173.14.233	UDP	Sounce	port:	10197	Destination	port:	29211
75.15.147.68		UDP	Sounce	port:	27208	Destination	port:	10197
	218.164.224.87	UDP	Sounce	port:	10197	Destination	port:	27171
68.173.14.233		UDP	Source	port:	29211	Destination	port:	10197
	68.173.14.233	UDP	Source	port:	10197	Destination	port:	29211
75.15.147.68		UDP	Sounce	port:	27208	Destination	port:	10197
75.15.147.68		UDP	Sounce	port:	27208	Destination	port:	10197
75.15.147.68		UDP	Source	port:	27208	Destination	port:	10197

### Architecture evolution

- Changes in the compression and encryption
  - data is still encrypted with RC4 and the XOR byte-with-preceding-byte + another added layer: a byte-per-byte XOR applied to each block of the configuration

https://www.symantec.com/connect/blogs/zeusbotspyeye-p2p-updated-fortifying-botnet

### Architectures: client-server

- Centralized architecture
- built on Internet Relay Chat or by using Domains or Websites (HTTPS)
- The Bots connect to one or more server through one or more domains.
- C&C is the SPF. Easily to takedown
- The botmaster need to set up another C&C and redirect the domain to it.
- To take down this botnet, it would be required to suspend all domains associated or to seize the domain and point it to a functional server (sinkhole) in order to keep the bot away from the legit C&C.
- <u>Rustock botnet</u> and <u>Srizbi botnet</u>



### Architectures: P2P

- Decentralized Botnet Architecture
- Provides <u>resiliency against network failures</u> in the botnet
- Try to solve the problem of authorities targeting domains or server
- Properties:
  - The bots are not (necessarily) connected to C&C server
  - Bots are connected in a mesh network in which the commands are send from Zombie to Zombie
  - Each nodes mantains a list of IP addresses of other nodes "neighbor" with which they communicate and exchange commands
  - Commanders can be identified just through secure keys, and all data except the binary itself can be encrypted.

### Architectures: P2P

- Every peer in the botnet can act as a C&C server, while none of them really are one.
- Bots are now capable of downloading commands, configuration files, and executable from other bots — every compromised computer is capable of providing data to the other bots,
- The new trend in the development of botnet is to provide them the capability to be "independent" from control servers, surviving and becoming



ny machines.

Tracking systems such as <u>ZeusTracker</u> are not able to track this variant due the impossibility to add the complete list of components of a P2P network instead only the IP addresses of C&C servers.

### **TOR Botnet**

- In September 2012 the German security firm <u>G Data Software</u> detected Skynet, a TOR-based botnet
- Dannis Brown at DefCon18 [4] has shown, for the first time, a possible implementation of a C&C channel over Tor to provide C&C server anonymity
- all critical communications of Skynet to its C&C servers are tunneled through a Tor SOCKS proxy running locally on compromised computers.

Even though Tor provides such an anonymity service, it also exposes the botnet activity due to recognizable patterns

•The server is anonymous and thus cannot point to the botnet owners' identity.

•The server cannot be taken down easily.

•The traffic is encrypted by Tor, so it can't be blocked by Intrusion Detection Systems.

•Tor traffic usually cannot be blocked altogether, because there are also legit use cases for Tor.

•The bot creator does not necessarily have to generate a custom protocol, but can use the known and reliable IRC protocol.



- Botnet Architecture evolved over time
- Advanced topology is more resilient to shutdown, enumeration or discovery

### Approaches to detection & measurement of botnets

- Passive Techniques
  - Packet Inspection
  - Analysis of Flow Records
  - DNS-based Approaches
  - Analysis of Spam
  - Analysis of Log Files
  - Honeypots
  - Evaluation of AV Feedback

- Active Techniques
  - Sinkholing
  - Infiltration
  - DNS Cache Snooping
  - Tracking of Fast-Flux Networks
  - IRC-based detection & monitoring
  - Enumeration of Peer-to-Peer Networks

### Tracking of Fast-Flux Networks

- Fast flux is a DNS technique used by <u>botnets</u> to hide <u>phishing</u> and <u>malware</u> delivery sites behind an ever-changing network of compromised hosts acting as proxies.
- The goal of fast-flux is for a fully qualified domain name (such as www.example.com) to have multiple (hundreds or even thousands) IP addresses assigned to it.
- These IP addresses are swapped in and out of flux with extreme frequency, using a combination of round-robin IP addresses and a very short Time-To-Live (TTL) for any given particular DNS Resource Record (RR)
- Fast-flux "motherships" are the controlling element behind fastflux service networks, and are similar to the command and control (C&C) systems found in conventional botnet



## Sinkholing

- Sinkholing is a technique that researchers use to redirect the identification of the malicious command-and-control (C&C) server to their own analysis server.
- Some of the larger botnets have been made unusable by TLD sinkholes that span the entire Internet

During 2012 Microsoft was running the sinkhole for the 70,000 malicious subdomains, it blocked more than 609 million connections from more than 7,650,000 unique IP addresses to the bad 3322.org subdomains. Legitimate subdomains were provided DNS service.

### Mirai Botnet



- IoT (non conventional) Botnet, mostly CCTV camera
- Mirai propagates by bruteforcing telnet server with a list of 62 default password
- Mirai is capable of launching multiple types of DDoS attacks, including SYNflooding, UDP flooding, Valve Source Engine (VSE) query-flooding, GRE-flooding, ACK-flooding (including a variant intended to defeat intelligent DDoS mitigation systems, or IDMSes), pseudo-random DNS label-prepending attacks (also known as DNS 'Water Torture' attacks), HTTP GET attacks, HTTP POST attacks, and HTTP HEAD attacks
- In early October, Mirai's developer released the malware's source code
- The researchers also note that the botnet's command and control (C&C) code is coded in Go, while the bots are coded in C
- Mirai was found to include a list of IPs that bots should avoid scanning: the US Postal Service, the Department of Defense, the Internet Assigned Numbers Authority (IANA) and IP ranges belonging to Hewlett-Packard and General Electric

### Mirai Botnet

 On October 21, Dyn received a global distributed denial of service (DDoS) attack on its DNS infrastructure on the east coast starting at around 7:10 a.m. ET (11:10 UTC).



### Zeus: A case study

- In October 2010 the US <u>FBI</u> announced that hackers in <u>Eastern Europe</u> had managed to infect computers around the world using Zeus.<sup>IBI</sup> The virus was distributed in an e-mail, and when targeted individuals at businesses and municipalities opened the e-mail
- In 2013 Hamza Bendelladj, known as Bx1 online, was arrested in Thailand III and deported to <u>Atlanta, Georgia</u>, USA.

### Zeus: A case study

- Zeus, also known as ZBot/WSNPoem, is famous for stealing banking information by using man in the browser keystroke logging and form grabbing
- The ZBot functions by downloading an encrypted configuration file and storing it in the location marked above. The Trojan opens up a backdoor connection for downloading/uploading from the command and control server, such as newer versions of configuration file, pushing the stolen data to a specific location as in the configuration file, etc
- any form of credentials or banking information is intercepted by it and uploaded to the secret location. It uses advanced mechanisms for form grabbing that sets up web pages and the user unknowingly enters his financial information,

### Zeus: A case study



Non- istate: 11.03.2009 me: 09:26:39 sit nary       Filter       Countries: Botnets: Dentes: Countries: Botnets: Dentes: Countries: Botnets: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes: Dentes:				
ite: 11.03.2009 me: 09:26:39       Countries: Countries: Botnets: e commands       Country: Pris: Type: Outside NAT ▼ Appi         me bots e commands       Forward >>         Meth template led files       2 fc_000ebbb       1.1.1.0/main 213				
te: 10:2.209 ne: 09:26:39 a ary Type: Outside NAT ( Appl Type: Ou				
Botnets:       JP's:         Type: Outside NAT & Appl         Type: Outside NAT & Appl         Porward >>         Result:         Image: Colspan="2">Porward >>         Porward >>         S         Result:         Porward >>         Porward >>         S         Porward >>         S         Porward >>				
ry e bots commands  New th template ad files  New th template d files  New th template d files  New the template ad files  New to the template ad template ad files  New to template a				
ry (r, commands)  Result: rommands  Result: (CompTID)  Ver/Botnet IP Country Socks Proxy Uuser_Id9ce10c45_01d6e996 1.1.1.0/main 2135 RU 213 38345 213  Result: (CompTID)  Ver/Botnet IP Country Socks Proxy Uuser_Id9ce10c45_01d6e996 1.1.1.2./main 94.1 94.1 1025 94  66.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  76.2  77.2  76.2  77.2  76.2  77.2  77.2  77.2  77.2  77.2  77.2  77.2  77.2  77.2  77.2  77.2  77.2  77.2  77.2  77.2  77.2  77.2  77.2  77.2  77.2  77.2  77.2  77.2  77.2  77.2  77.2  77.2  77.2  77.2  77.2  77.2  77.2  77.2  77.2  77.2  77.2  77.2  77.2  77.2  77.2  77.2  77.2  77.2  77.2	dy			
e bats commands         Envard >>           with template ad files         Image: 1045_01046_0996         1.1.1.0/main 2135 RU         213.138845         213.138845         213.138845         213.138845         213.138845         213.138845         213.138845         213.138845         213.138845         213.138845         213.138845         213.138845         213.138845         213.138845         213.138845         213.138845         213.138845         213.138845         213.138845         213.138845         213.138845         213.138845         213.138845         213.138845         213.138845         213.138845         213.138845         213.138845         213.138845         213.138845         213.138845         213.138845         213.138845         213.138845         213.138845         213.138845         21438845         213.1288456         113.227main 95         94.1288456         11025         94.1288456         214288456         214288456         214288456         214288456         214288456         214288456         214288456         214288456         214288456         214288456         214288456         214288456         214288456         214288456         214288456         214288				
Forward >>           commands           ath template           d files         I user_1d9ce1oc45_01d6e996           1.11.0/main 213.         5 RU         213.2         38345         213.2           3 family_01207eeb         1.11.2/main 97.         68         86.2         1027         86.2           3 family_01207eeb         1.12.2/main 97.         68         87.2         1025         -           4 d71952j_0019064f         1.12.2/main 97.         68         87.2         1025         -           6 illusion_f2243e_00576c9d         1.12.2/main 97.         68         82.1         1025         -           7 brian_ally_0228d16c         1.12.2/main 82.         68         82.4         11025         -           9 your_jaxxijzedk_00a304bc         1.12.2/main 82.         68         82.4         11025         -           10 home_881b31b48d_00170f87         1.12.2/main 85.         TH         58.5         1025         -           11 your				
commands         Result:         # [Comp10         Ver/Botnet         1P         Country         Socks         Proxy           1 user_id9ce10c45_01d6e996         1.1.1.0/main 2135         RU         21358245         2135           2 fic_000eb9b         1.1.2.2/main 94.1          94.1         210.25         884.5           3 family_01207eeb         1.1.2.2/main 95         GB         86         1025         94           4 d719sf2j_0019064f         1.1.2.2/main 195.         RU         195         1025         1025           5 218_u_l_00a3738         1.1.2.2/main 195.         RU         195         1025         1025           7 brian_ally_0228d16c         1.1.2.2/main 195         RU         195         1025         10           9 your_jaxxytack_00b03000         1.1.2.2/main 94          94.1         1025         10           10 home_881b31b48d_00170f87         1.1.2.2/main 58         TH         58         1048         58           11 your				
Result:         Country         Socks         Proxy           # Complo         Ver/Botnet         1P         Country         Socks         Proxy           # Complo         1.11.0/main 213.         5 RU         213.2         38345         213.1         38345         213.1         38345         213.1         38345         213.1         38345         213.1         38345         213.1         38345         213.1         38345         213.1         38345         213.1         38345         213.1         38345         213.1         38345         213.1         38345         213.1         38345         213.1         38345         213.1         38345         213.1         38345         213.1         38345         213.1         38345         213.1         38345         213.1         38345         213.1         38345         213.1         38345         213.1         38345         213.1         38345         213.1         38345         213.1         38345         213.1         38345         213.1         22.2         68         82.1         38345         213.1         22.2         38345         213.1         22.2         38345         213.1         22.2         38345         213.1         22.2         38345				
#// Comp10         Ver/Botnet         IP         Country Socks         Proxy           1 user_1d9ce10c45_01d6e96         1.1.1.0/main 213.         RU         213.1         28345         213.1           4 driles         fic_000ebbb         1.1.2.2/main 94.1         -         94.1         1027         94.1           3 family_01207eeb         1.1.2.2/main 85.1         GB         86.1         1027         86.2           4 dr19sf2j_0019064f         1.1.2.2/main 85.1         GB         86.1         1025         1.5           5 218_u_1_00a:2738         1.1.2.2/main 195         RU         19         1025         1.5           6 illusion_f2243e_00576c9d         1.1.2.2/main 124         TH         124.1         114         124.1         11025         4           9 your_jaxvijzedk_000364bc         1.1.2.2/main 82         GB         82.1         11025         4           11 your				
1       user_iddcc10c45_01d6e996       1.11.10/main 2135 RU       213.1238345       213.1238345         2       fic_000eb9b       1.1.2.2/main 94.1       -       94.19       94.1		Screenshot I	Kill OS Online tin	ne Lag
2 fic_000ebb9b       1.1.2.2/main 94.1        94.1       94.1       94.1       94.1         3 family_01207eab       1.1.2.2/main 95.1       GB       86.1       1027       86.2         4 d719sf2_0019064f       1.1.2.2/main 97.5       GB       87.2       86.1       1027       86.2         5 218_u_1_00ac3738       1.1.2.2/main 195       RU       192.5       11025       195.2         6 illusion f2243e_00576c9d       1.1.2.2/main 195       RU       192.5       1027       8         7 brian_ally_0228d16c       1.1.2.2/main 195       RU       192.5       1027       -         10 home_8815b48d_0017067       1.1.2.2/main 94        94.11       1025       94.11         11 your	:10051	. View H	Kill 96:13:3	39 0.9
3 family_01207ceb       1.1.2.2/main 86.1       GB       86.1       1027       86.1         4 d719sf2j_0019064f       1.1.2.2/main 87.1       GB       87.24471025       -         5 218_u_l_00ac3738       1.1.2.2/main 195       RU       19       1025       155.1         6 illusion_f2243e_00576c9d       1.1.2.2/main 124       TH       124.1       11025       -         7 brian_ally_022801c       1.1.2.2/main 82       GB       82.1       1025       94.1         9 your_jaxvxjzedk_000364bc       1.1.2.2/main 82       GB       82.1       1048       58.5         10 home_881b31b48d_00170f97       1.1.2.2/main 85       TH       58.5       1048       58.5       54.5         12 blackxp_000325d8       1.1.2.2/main 75.       RU       77.5       77.5       52.5       14.1       124.1       14.1       124.1       14.1       124.1       14.1       124.1       14.1       124.1       14.1       124.1       124.1       124.1       124.1       124.1       124.1       124.1       124.1       124.1       124.1       124.1       124.1       124.1       124.1       124.1       124.1       124.1       124.1       124.1       124.1       124.1       124.1       124.1 </td <td>34451</td> <td>View I</td> <td>Kill 96:32:4</td> <td>47 0.7</td>	34451	View I	Kill 96:32:4	47 0.7
4 d719sf2j_0019064f       1.1.2.2/main 87.       GB       87.26.47.1025       -         5 218_u_l_00a23738       1.1.2.2/main 195.       RU       197.26.47.1025       195.27.26.17.1025         6 illusion_f2243e_00576c9d       1.1.2.2/main 192.       GB       82.12.27.1025       -         7 brian_ally_0228d16c       1.1.2.2/main 82.       GB       82.12.27.1025       -         9 your_jaxxyizedk_00364b       11.2.2/main 84.        94.11.025.1025       -         10 home_881b31b48d_0017067       1.1.2.2/main 58.       TH       58.27.1025       -         11 your	22093	View H	Kill 98:58:4	44 0.3
5 218_u_1_00ac3738       1.1.2.2/main 195       RU       19900000000000000000000000000000000000		View I	Kill 96:49:0	07 0.2
6 illusion_f2243e_00376c9d       1.1.2.2/main 124.       TH       124	10359	View H	Kill 96:27:0	06 0.1
7         brian_ally_0228d16c         1.1.2.2/main 82		View I	Kill 104:12:	36 0.8
8 telekit_7482b02_00b07900       1.1.2.2/main 94        94.1100000000000000000000000000000000000		View H	Kill 97:49:	55 0.3
9 your_jaxvxjzedk_00a364bc       1.1.2.2/main 82GB       82.2.2.2.7.7:1025         10 home_881b31b480_00170F0       1.1.2.2/main 58       TH       58.5.2.1048       58.5.2.1048         11 your11.2.2/main 58       TH       58.5.2.1048       58.5.2.1048       58.5.2.1048         12 blackxp_000325d8       1.1.2.2/main 12       TH       -       124.1.2.1         13 b154bc1afca840e_00397f1d       1.1.2.2/main 77       RU       77.5.2.71027       77.5.2.2         14 xp_0051dba0       1.1.2.2/main 77       RU       77.5.2.71027       77.5.2.2         15 desktop_02659af2       1.1.2.2/main 78       TH       58.5.2.1025       190.1.5.2         16 davie_0085eb43       1.1.2.2/main 92        92.1.2.5.1025       93.1.2.2         19 microsof. 886ba_01b17ree       1.1.2.2/main 92        92.1.2.5.2.1025       92.1.2.2         19 microk_0069abc       1.1.2.2/main 193       SK       193.6.2.1025       93.5.2.1025       92.1.2.2         20 ammo_00135651       1.1.2.2/main 82       GB       86.2.1027       -       22       pc_fec662b1943d_00153eaa       1.1.2.2/main 85.2	59:33846	View I	Kill 98:00:4	42 0.1
10 home_881b31b48d_00170f87       1.1.2.2/main 58		View 1	Kill 96:10:2	44 26
11 your	32353	View	Kill 103:14:	13 1.0
12 blackxp_000325d8       1.1.2.2/main 12       TH       -       124.2         13 b154bc1afca840e_00397f1d       1.1.2.2/main 77       RU       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77.5       77	17992	View P	Kill 104:12:/	03 0.5
13 b154bc1afca840e_00397f1d       1.1.2.2/main 77.       RU       77.5       77.5         14 xp_0051dba0       1.1.2.2/main 58.       TH       58.5       1025       58.5         15 desktop_02659af2       1.1.2.2/main 58.       TH       58.5       1025       190.5         16 davie_0085eb43       1.1.2.2/main 62       GB       62.5       1036       62.5         17 1_d07192a7a4944_0025f97       1.1.2.2/main 95.        95.5       95.5       95.5         18 microsof_886bea_01bd77ea       1.1.2.2/main 92.        92.15       95.5       95.5         19 mircik_00069abc       1.1.2.2/main 193.       SK       193.5       1025       193.5         20 ammo_0013561       1.1.2.2/main 82.       GB       82.5       1025       82.3         21 freedom_867dc59_000050cf       1.1.2.2/main 82.       GB       86.5       1027       -         22 pe_fec662b1943d_00153eae       1.1.2.2/main 82.       GB       86.5       1027       -         23 pen_0030760       1.1.2.2/main 95.        95.5       54537       24.4       1027       -         25 basftpz_7e2bb74_017743b0       1.1.2.2/main 89.       FU       89.5       54537       24.4       1025 <td< td=""><td>47:37760</td><td>-</td><td>- 98:38:</td><td>15 0.1</td></td<>	47:37760	-	- 98:38:	15 0.1
14 xp_0051dba0       1.1.2.2/main 58.       TH       58.       1025       58.         15 desktop_02659af2       1.1.2.2/main 190       AR       190.5       1025       190.5         16 davie_00085eb43       1.1.2.2/main 190       AR       190.5       1036       62.3       1036       62.3       1037       1025       190.5       1025       190.5       1036       62.3       1036       62.3       1036       62.3       1036       62.3       1036       62.3       1036       62.3       1036       62.3       1036       62.3       1036       62.3       1036       62.3       1036       62.3       1036       62.3       1036       62.3       1036       62.3       1036       62.3       1036       62.3       1036       62.3       1036       62.3       1036       62.3       1036       62.3       1036       62.3       1036       62.3       1036       62.3       1036       62.3       1036       62.3       1036       62.3       1037       1036       62.3       1025       1037       105       1027       105       1027       105       1027       105       1027       105       1027       105       1027       1027       1036	27:14804	View I	Kill 104:11:	25 0.0
15       desktop_02659af2       1.1.2.2/main 190       AR       190.1       1025       190.1         16       davie_0085eb43       1.1.2.2/main 62       GB       62.2       1036       62.2         17       1_d07192a7a4944_0025f597       1.1.2.2/main 95        92.1       1026       62.2         18       microsof_886bea_01bd7ea       1.1.2.2/main 95        92.1       51.025       92.1         19       micik_00069abc       1.1.2.2/main 193       SK       193.6       1025       92.1         20       ammo_00135651       1.1.2.2/main 82       GB       82.2       1025       82.2         21       freedom_867dc59_00050cf       1.1.2.2/main 82       RU       82.2       1027       -         22       pc_fec662b1943d_00153eae       1.1.2.2/main 85       GB       86.2       1027       -         23       pen_003f0760       1.1.2.2/main 85        95.2       51025       95.2       51025         24       home	=37112	View	Kill 97:37:	17 3.9
16 davie_0085eb43       1.1.2.2/main 62       6B       62       1036       62.         17 1_d07192a7a4944_0025f97       1.1.2.2/main 95.        95.1       95.1       95.1         18 microsof_886bea_01bd77ea       1.1.2.2/main 95.        95.1       95.1       95.1         19 micrik_00069abc       1.1.2.2/main 193.       SK       193.6       1025       193.5         20 ammo_00135651       1.1.2.2/main 82.       GB       82       1025       82.3         21 freedom_867dc59_000050cf       1.1.2.2/main 82.       GB       86       1027       -         22 pc_fcc662b1943d_00153eaa       1.1.2.2/main 95.        95.2       95.2       95.2         24 home       1.1.2.2/main 95.        95.2       95.2       95.2       95.2         24 home       1.1.2.2/main 95.        95.2       95.2       95.2       95.2       95.2       95.2       95.2       95.2       95.2       95.2       95.2       95.2       95.2       95.2       95.2       95.2       95.2       95.2       95.2       95.2       95.2       95.2       95.2       95.2       95.2       95.2       95.2       95.2       95.2       95.2	18:32639	View	Kill 107:20:	49 0.6
17       1.11.2./main 92        95.1       95.1       95.1         17       1.12.2./main 92        95.1       95.1       95.1         18       microsof_886bea_01bd77ea       1.1.2.2/main 92        92.1       95.1       1025       95.1         19       micric_00069abc       1.1.2.2/main 92        92.1       95.1       1025       93.2         20       ammo_00135651       1.1.2.2/main 82       GB       82       1025       82.3         21       freedom_867dc59_000050cf       1.1.2.2/main 82       RU       82.2       1027       -         22       pc_fec662b1943d_00153eae       1.1.2.2/main 96       GB       86       1027       -         23       pen_003f0760       1.1.2.2/main 95        92.2       1025       89.2         24       home	37719	View	Kill 96:34:	49.0
18       microsof. 886bea_01b17/se       1.1.2.2/main 932		View	Vill 100(52)	11 2 2
13       micride_00069abc       1112.2/main 192       54.       102.3       54.         19       micride_00069abc       11.2.2/main 193       54.       193.       102.3       193.       102.3       193.       102.3       193.       102.3       193.       102.3       102.3       1102.3       1102.3       1102.3       1102.3       1102.3       1102.3       1102.3       1102.3       1102.3       1102.3       1102.3       1102.3       1102.3       1102.3       1102.3       1102.3       1102.3       1102.3       1102.3       1102.3       1102.3       1102.3       1102.3       1102.3       1102.3       1102.3       1102.3       1102.3       1102.3       1102.3       1102.3       1102.3       1102.3       1102.3       1102.3       1102.3       1102.3       1102.3       1102.3       1102.7       1102.3       1102.7       1102.7       1102.7       1102.7       1102.5       1102.5       1102.5       1102.5       1102.5       1102.5       1102.5       1102.5       1102.5       1102.5       1102.5       1102.5       1102.5       1102.5       1102.5       1102.5       1102.5       1102.5       1102.5       1102.5       1102.5       1102.5       1102.5       1102.5       1102.5	10303	Manu	Kill 96:36:	01 2 7
13 mircle_0003800       11.12.2/main 832       Six       13.11.12.2       Six       13.11.12.2       13.11.12.2         20 ammo_00135651       11.12.2/main 82.       Six       88       82.11.12.2       88.11.12.2         21 freedom_867dc59_000050cf       1.1.2.2/main 82.       RU       82.11.11.12.7       -         22 pc_fcc62b1943d_00153eae       11.12.2/main 86.       Six       88       86.11.027       -         23 pen_003f0760       1.1.2.2/main 95.        95.11.025       95.11.025       95.11.025       95.11.025       89.11.025       89.11.025       89.11.025       89.11.025       89.11.025       89.11.025       89.11.025       89.11.025       89.11.025       89.11.025       89.11.025       89.11.025       89.11.025       89.11.025       89.11.025       89.11.025       89.11.025       89.11.025       89.11.025       89.11.025       89.11.025       89.11.025       89.11.025       89.11.025       89.11.025       89.11.025       89.11.025       89.11.025       89.11.025       89.11.025       89.11.025       89.11.025       89.11.025       89.11.025       89.11.025       89.11.025       89.11.025       89.11.025       89.11.025       89.11.025       89.11.025       89.11.025       89.11.025       89.11.025       89.11.025       89.11.0	22664	View 1	Vill 96:41.0	51.0.1
20 ammio_00133071       1.12.2/main 82.       80       82       1.02.7       92         21 freedom_867dc59_000050cf       1.12.2/main 86.       RU       82       81       1027       -         22 pc_fec662b1943d_00153eae       1.12.2/main 86.       GB       86.       1027       -         23 pen_003f0760       1.12.2/main 95.        95.       95.       95.       95.       95.         24 home       1.12.2/main 85.        95.       95.       95.       95.       95.       95.         25 bsaftpz_7e2b574_017743b0       1.12.2/main 89.       HU       89.       95.       95.       95.       95.       95.       95.       95.       95.       95.       95.       95.       95.       95.       95.       95.       95.       95.       95.       95.       95.       95.       95.       95.       95.       95.       95.       95.       95.       95.       95.       95.       95.       95.       95.       95.       95.       95.       95.       95.       95.       95.       95.       95.       95.       95.       95.       95.       95.       95.       95.       95.       95.	2004	Manu	Kill 06:21:	50.1
21 freedom_do/dc3g/d00030cr       11.2.2/main 82.       KD       62.       1102/       -         22 pc_fcc62521043d_00153ea       11.2.2/main 82.       GB       86.       1027       -         23 pen_003f0760       11.2.2/main 95.        95.       95.       95.       95.         24 home	:13365	view r	xiii 90:31:.	10 0.1
22 pc_recoord/9430_001364a       1112.2/main 85       58       58       50       1027         23 pc_n003f0760       11.2.2/main 85        95       95       95       95         24 home       11.2.2/main 24       24       54537       24.4       54         25 bsaftpz_re2b574_017743b0       11.2.2/main 89       HU       89       51025       89         26 client_df77fa69_0d6210d8       11.2.2/main 89       RO       89       1025       89         27 accr_d430879900_004dbc2a       11.2.2/main 89       TH       -       202       715         28 abc_67365a4e5b6_00204191       11.2.2/main 11       TH       115       1027       115		View /	xill 104.11.	20 0.0
23 pen_0030700       1.1.2./main 95.        95.        1023       95.         24 home		view /	104:11:2	10 0.1
24 nome         11.2.2/main 89         24         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14 <td>31003</td> <td>view P</td> <td>XIII 96:39:4</td> <td>22 0.3</td>	31003	view P	XIII 96:39:4	22 0.3
25 bsattp2_re2bb74_01/r43b0         1.1.2.2/main 89.         H0         89.         11025         89.           26 client_df77fa69_0d6210d8         1.1.2.2/main 89.         RO         89.         1025         89.           27 acer_4d30879900_004dbc22         1.1.2.2/main 20.         TH         202.         20.         115.         1027         115.         1027         115.         1027         115.         1027         115.         1027         115.         1027         115.         1027         115.         1027         115.         1027         115.         1027         115.         1027         115.         1027         115.         1027         115.         1027         115.         1027         115.         1027         115.         115.         1027         115.         1027         115.         1027         115.         1027         115.         1027         115.         1027         115.         1027         115.         1027         115.         1027         115.         1027         115.         115.         1027         115.         1027         115.         115.         115.         115.         115.         115.         115.         115.         115.         115.         115. <t< td=""><td>(27755</td><td>View 1</td><td>xiii 104:12:2</td><td>37 U.E</td></t<>	(27755	View 1	xiii 104:12:2	37 U.E
26 cment_df7/fa09_0d6210d8 1.1.2.2/main 89. RO 89. 1025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 89. 2025 8	18514	view	xiii 97:55:1	18 0.2
27 acer_4d308/9900_004dbca2 1.1.2.2/main 20 TH - 202. 28 abc_67365a4e5b6_00204191 1.1.2.2/main 11 15.	\$:38462	view H	xiii 96:14:1	16 0.7
28 abc_67365a4e5b6_00204191 1.1.2.2/main 11 115. 115. 115. 1127 115.	2:25983		97:16:	110
	34129	View H	Kill 98:45:2	29 8.4
29 skz_td19c55e0a2_003d5664 1.1.2.2/main 61. TH 61.5 1025 61.5 51.0 51.5 51.5 51.5 51.5 51.5 51.5 5	35502	View H	Kill 96:32:3	12 10.

Fert

### Zeus Botnet

Some of the features that this botnet displays are:

- •Captures credentials over HTTP, HTTPS, FTP, POP3
- •Steals client-side X.509 public key infrastructure certificates
- Has an integrated SOCKS proxy
- •Steals/deletes HTTP and flash cookies
- •Captures screenshots and scrapes HTML from target sites
- •Modifies the local hosts file
- •Groups the infected user systems into different botnets to distribute command and control
- •Has search capabilities which may be used through a web form
- The configuration file is encrypted
- •Has a major function to kill the operating system
- Contacts command and control server for additional tasks to perform
- Has a unique bot identification string

•Sends a lot of information to C&C server, such as the version of the bot, operating system, local time, geographic locations, etc.

#### Black Atlas botnet to deliver PoS malware



- Black Atlas was targeted at small and medium-sized businesses with the goal of breaking into their networks and ultimately stealing data from point-of-sale terminals
- It includes brute-force tools for guessing passwords, SMTP (email) scanners and remote desktop scanners, among other tools.
- It can deliver advanced malware such as BlackPOS, which is best known for the pivotal role it played in the theft of approximately 40 million payment cards from retailer Target in late 2013.
- Finally, it can exfiltrate the data it captures, using HTTP POST.
- Black Atlas is a good example of how the most effective botnets can piece together different tools and techniques to take advantage of weak network defenses

### Black Atlas: A case study

Cybercriminals use pen testing tools, including brute force attacks, to gather information about networks.



Upon gaining access, cybercriminals use a second batch of tools to get further inside. Cybercriminals familliarize themselves with the environment then installs PoS threat, including the modular malware Gorynych. Cybercriminals gather dumped financial and other data.

### Black Atlas: A case study

 Black Atlas operators used the modular botnet Gorynych or Diamond Fox in some installations. Gorynich was used to download a repurposed BlackPOS malware with RAM scraping functionality and upload all the dumped credit card numbers in memory. As the original BlackPOS used a text file to store pilfered credit card data, Gorynych now grabs that text file and does an HTTP POST to complete the data exfiltration