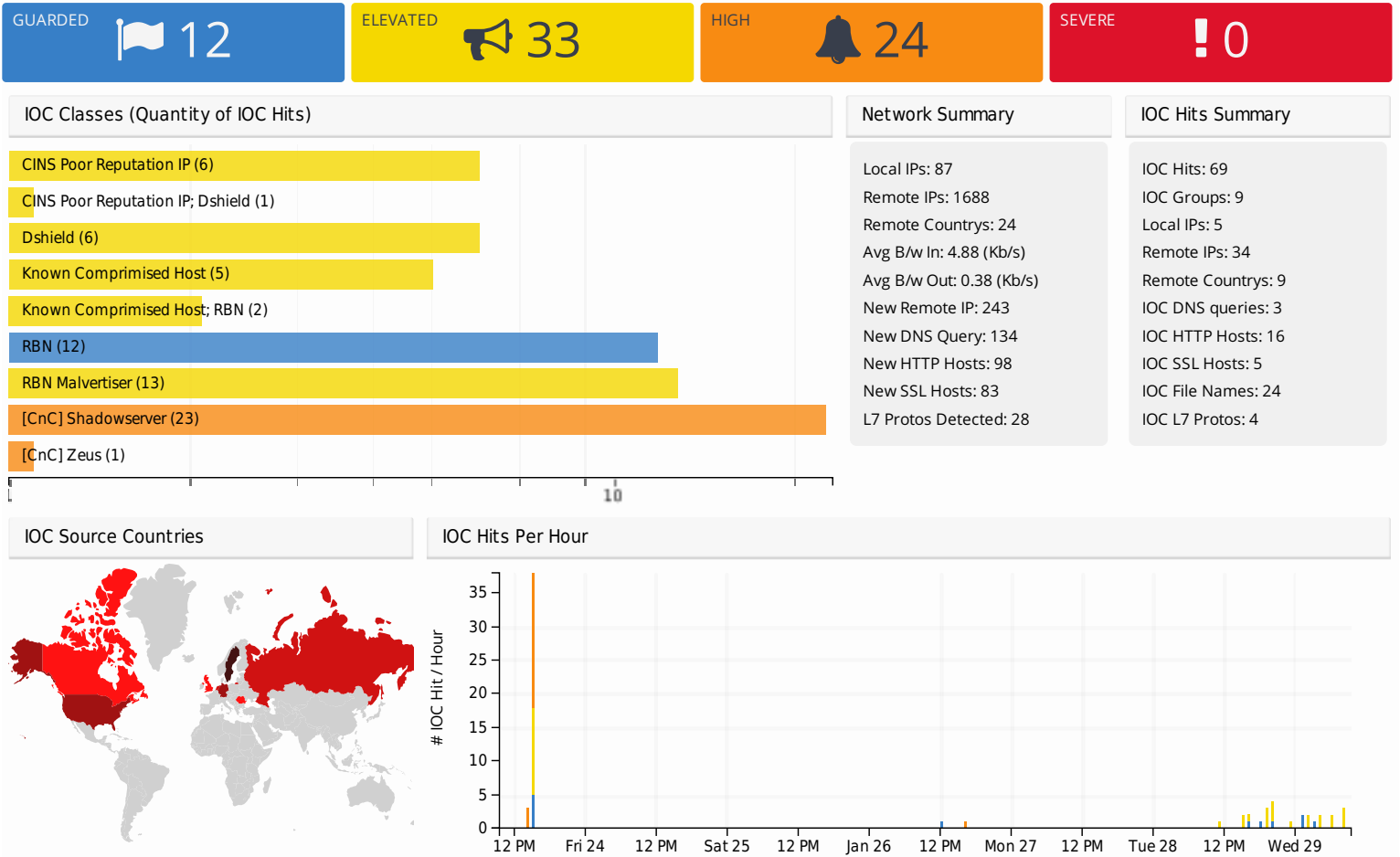

















This report summarizes rapidPHIRE's detection of Indicators of Compromise - IOC - (i.e. network communications between users and known malicious hosts, files or entities). These events have occurred within one or more data network zones within your organization. It should be noted that some IOC detection events are merely points of concern (e.g. Tor exit node detected) whereas others can be more conclusive in nature and may require immediate remediation (e.g. malicious file downloaded by user). The following bar chart below plots the number of unique IOC detection events occurring within one hour time-slices inside the date range indicated in the upper right corner of this page.



The tables below are aggregated lists of IOC events, grouped by IOC Name, IOC Type and LAN IP / Remote IP pairing. Each row that is displayed may contain one or more distinct connection events. A count of unique events is provided. For example, a user may repeatedly browse to a known malvertiser website. This activity would be displayed as a single entry showing a count of the number of unique connections to that site. Security administrators should access the rapidPHIRE GUI to view any listed IOC event records in more detail.

Top Remote IP Addresses Triggering IOC Notifications						
Last Seen		IOC Hits	IOC	IOC Type	Remote Country	
2014-01-23 15:52:08		23	[CnC] Shadowserver	IP Address	Romania	
2014-01-23 15:52:52		13	RBN Malvertiser	IP Subnet	United States of America	
2014-01-29 03:00:42		12	RBN	IP Subnet	Sweden	
2014-01-29 08:41:27		6	CINS Poor Reputation IP	IP Address	Germany	
2014-01-29 06:56:03		6	Dshield	IP Subnet	Netherlands	
2014-01-29 08:20:05		5	Known Comprised Host	IP Address	China	
2014-01-28 20:31:15		2	Known Comprised Host; RBN	IP Address;	Russia	
2014-01-26 16:06:55		1	[CnC] Zeus	IP Address	Canada	
2014-01-29 06:02:51		1	CINS Poor Reputation IP; Dshield	IP Address;	United States of America	

Local End Point IP Addresses Triggering IOC Hits

Last Seen		IOC Hits	IOC	IOC Type	LAN IP	WAN IP	Lan Zone	
2014-01-23 15:52:08		23	[CnC] Shadowserver	IP Address	192.168.0.189	-	Dev	↑↓
2014-01-23 15:52:52		13	RBN Malvertiser	IP Subnet	192.168.0.112	-	Corporate	↑↓
2014-01-23 15:21:48		5	RBN	IP Subnet	192.168.0.245	-	Dev	↑↓
2014-01-29 01:56:15		5	RBN	IP Subnet	69.196.159.67	-	DMZ	↑↓
2014-01-29 08:20:05		4	Known Comprimised Host	IP Address	69.196.159.67	-	DMZ	↑↓
2014-01-29 08:41:27		4	CINS Poor Reputation IP	IP Address	69.196.159.67	-	DMZ	↑↓
2014-01-29 06:56:03		3	Dshield	IP Subnet	69.196.159.67	-	DMZ	↑↓
2014-01-29 02:02:32		3	Dshield	IP Subnet	69.196.159.68	-	DMZ	↑↓
2014-01-28 19:51:55		2	CINS Poor Reputation IP	IP Address	69.196.159.68	-	DMZ	↑↓
2014-01-28 20:31:15		2	Known Comprimised Host; RBN	IP Address;	69.196.159.67	-	DMZ	↑↓
2014-01-26 12:06:11		1	RBN	IP Subnet	192.168.0.112	-	Corporate	↑↓
2014-01-26 16:06:55		1	[CnC] Zeus	IP Address	192.168.0.112	-	Corporate	↑↓
2014-01-29 02:29:55		1	Known Comprimised Host	IP Address	69.196.159.68	-	DMZ	↑↓
2014-01-29 03:00:42		1	RBN	IP Subnet	69.196.159.68	-	DMZ	↑↓
2014-01-29 06:02:51		1	CINS Poor Reputation IP; Dshield	IP Address;	69.196.159.68	-	DMZ	↑↓

rapid

Glossary

RBN

The Russian Business Network (commonly abbreviated as RBN) is a multi-faceted cybercrime organization, specializing in and in some cases monopolizing personal identity theft for resale. It is the originator of MPack and an alleged operator of the now defunct Storm botnet.

The RBN, which is notorious for its hosting of illegal and dubious businesses, originated as an Internet service provider for child pornography, phishing, spam, and malware distribution physically based in St. Petersburg, Russia. By 2007, it developed partner and affiliate marketing techniques in many countries to provide a method for organized crime to target victims internationally.

IP address ranges from which the former customers of the RBN ISP, their malware marketing affiliate networks, emulators, and other organized crime groups exploit consumers. Block at will. Test for your production environment prior to utilization. In cases where a malicious domain occupies an IP address used by many domains, the IP address is not included in this list.

[CnC] Zeus

Zeus (also known as Zbot / WSNPoem) is a crimeware kit, which steals credentials from various online services like social networks, online banking accounts, ftp accounts, email accounts and other (phishing). Zeus can capture credentials out of HTTP-, HTTPS-, FTP- and POP3-traffic or out of the bot's protected storage (PStore).

The Zeus trojan spreads on email as well via drive-by infections (using toolkits like LuckySploit, El fiesta and so on). It's the decision of the cybercriminal how he would like to distribute the binary.