# proofpoint.

# Emerging Threats Intelligence Features and Usage

# Windows User

# Registration

New users of ET Intelligence Query will need to register for an account at https://etadmin.proofpoint.com. The user will need to supply Proofpoint Emerging Threats with basic information to complete the registration process. The user will be given the option of creating, or joining a current organization. If the user is joining a current organization, approval by that organization's portal admin must be obtained. The user will be asked to verify the email address supplied, and will be granted approval by the organization admin if necessary.

Once registered and approved the user will have access to the ET Intelligence Query button on the toolbar of the portal landing page.

# proofpoint. Home ETPro Ruleset ETOpen Ruleset ET Intelligence I Home Home API Access API Documentation My Account Notifications Reputation List Acces Organization Details There are current Reputation List Acces Subscriptions Search History Threat Intelligence P



The user will be presented with "API Access and Search Options." Clicking the API Access hyperlink will present the user with their API authorization key. ET Intelligence Query API functionality is not the focus of this document. API documentation can be found at the link below:

https://apidocs.emergingthreats.net/#introduction

The search portal has been updated to https://threatintel. proofpoint.com which features a redesigned user interface. You will automatically be redirected to this site or can access it directly using your ET credentials.

# **Information Search**

The ET Threat Intelligence Portal provides you with a powerful mechanism to search for different object types which you may have observed in your environment. Currently we offer five different searches in the search box.

- 1. IP Address: Simply enter the host IP address that you would like to search for in the search box. For example, 114.112.255.81
- 2. Domain: This would be the fully qualified domain name that you would like to evaluate the reputation of. Note that this is not a URL, but instead the base FQDN. For example, ilo.brenz.pl
- 3. Signature ID: Also known as SID, which is a term used for a rule identifier in Suricata and Snort. You can search for any ETPro or ET Open signature. For example, 2804682
- 4. SID Message Text: You can look for any text in the SID's to find any associated rules. This is an autocomplete function, so you can simply type any matching keywords to find. For example, "Angler".
- 5. MD5 Hash: This would be the MD5 for any sample which has been uploaded into the SensorNet/SandNet. Simply enter the MD5 hash for that sample: For example, 757782d6a88684b923aabbba62157205
- SHA256 Hash: This would be the SHA256 for any sample which has been uploaded into the SensorNet/SandNet. Simply enter the SHA256 hash for that sample: For example, 040bc6452ce4671032622ca4b1a602f3ab8fdcc63f953b01567db028db8677ae

Note that if you click upon the text box, a pop up will appear which lets you click on sample entries. So you can immediately look at entries which change over time.



Figure 2: ET Search

### **Time Range Selector**

Threats and actors change dramatically over time, and it is important to maintain the right context for researching how these impact your environment. The Time Range Selector gives you the power to view the threat landscape over different periods of time. The default timeframe is 30 days. The selector will not only impact what is displayed in the Reputation History Graph, but it also will impact what content is displayed for other areas. For instance, this will filter how far back IDS Events, Samples, Domains, and other content will be shown.

#### Viewing different time ranges:

ET Intelligence will score an event based upon the source, the confidence, and other factors such as the offending behavior. This gives an IP an initial reputation. If there is no other activity, then IP's reputation score will decay over a short period of time. If activity persists then there the reputation will be refreshed. This helps ensure that a machine that was compromised and then remediated will not be forever condemned, nor will that be the case for an IP or domain which may have been malicious at some point, but then cleaned up or repurposed. However it allows us to ensure that sources that are actively malicious are still properly represented.





Category         II         Sorre         IF         Frint Seen         II         Last Seen         II           I         Category         II         Sorre         IF         Frint Seen         II         Last Seen         II         Interview         <	Current Reputation         Reputation History           Category         11         Sorre         First Seen         11         Last Seen         1           ChatSarver         78         201242-13         20154948         1         140         100           Constrainer         0         000000000000000000000000000000000000	
✓         Category         II         Soure         IF         Frint Seen         II         Last Seen         II           ✓         ChatServer         78         2012-02-13         2015-08-08         II         500           ✓         Croc         0         2012-02-13         2015-06-02         100         100           ✓         First         0         2012-02-13         2012-02-02         100         100           ✓         First         0         2012-02-13         2012-02-03         2012-02-03         100           ✓         Spam         0         2012-02-13         2012-02-03         2012-02-03         2012-02-03	✓ Category         It         Score         IF         First Seen         II         Last Seen         II           ✓         ChatServer         78         2012/20:13         2015/09:08         100         100           ✓         ChatServer         78         2012/20:13         2015/09:08         100         100	
Image: Chardisenser     78     2012-02-13     2015-08-08       Image: Chardisenser     0     2012-02-13     2015-06-12       Image: Chardisenser     0     2012-02-13     2015-06-02       Image: Chardisenser     0     2012-02-13     2012-02-03       Image: Spam     0     2012-02-13     2012-02-03	ChatServer         78         2012-02-13         2015-08-08         120           Conc         0         2015-03-13         2015-08-08         100	
Image: Concolor of the system         0         2012-02-13         2015-06-12         50           Image: System         0         2012-02-13         2012-06-02         60         60           Image: System         0         2012-02-13         2012-06-02         60         60         60           Image: System         0         2012-02-13         2012-06-02         60 <td>Coc 0 2012/02/12 2016/06/12 100</td> <td></td>	Coc 0 2012/02/12 2016/06/12 100	
Image: P23P         0         2012-07-10         2012-08-02         00           Image: Sparm         0         2012-02-13         2012-04-03         40           20         20         20         20         20		
✓         Spam         0         2012-02-13         2012-04-03         40           20         20         20         20         20         20		
	☑ Sparm         0         2012-02-13         2012-04-03         40           ☑         ☑         ☑         ☑         ☑	

#### Figure 4: 90 Day Example

nt Reputatio	n				Reputation History	
Category	It Score I	First Seen	It Last Seen	u î		
ChatServer	78	2012-02-13	2015-09-08		120	
CnC	0	2012-02-13	2015-08-12		100	
P2P	0	2012-07-10	2012-08-02		80	
Spam	0	2012-02-13	2012-04-03		40	

Figure 5: Max Reputation History Example

Note that you can also click on the checkboxes in the Current Reputation Table to select what categories show up in the graph. This can be useful when there are multiple categories or you are only concerned with one type.



Figure 6: Max Reputation with Individual Category Selection

Anyone can produce a list of IP addresses. It's the story behind the list that is interesting—and most often missing. The goal of ET Intelligence Query is to stop the dead-end nature of most threat intelligence sources and illuminate all of the evidence behind why an IP address should be investigated in the first place. With the IP Search feature, we provide the needed context surrounding an IP going back historically as far as four years.

IP Reputation History can tell a detailed story of an IP addresses behavior and use over time. Often a combination of categories can identify with high fidelity: malicious actors, their tools, and their intentions.

IP IDS events provide a direct connection to IP Reputation history. The information within this section is where a category like CnC is expanded to include the malware family name, its protocol, and often its intention—all in the language of the ETPro and ETOpen rule set. The type of rules an IP address fires is one of the biggest factors in the assignment of reputation category.

Related samples and domains help close the loop in an investigation where information is missing. Maybe you have the sample, but need the call back IP addresses to stop or identify infection. Related data means that indicators of compromise (IOC) will only rarely be isolated.

Armed with this data, and the other information provided on the IP Address search page, the user will be able to see a detailed story behind each IP, relate it to many different IOCs, and get a better understanding of the risk presented by IP addresses in this ASN.

# **IP Address Search**

ET Intelligence Query allows the user to search for any public IPv4 address. The search will provide the historical ET view of an IP address object, and at the very least the ASN information for any IP. IP's with any reputation will also show a great deal of information.

The information is represented in a tabbed layout to help provide at a glance understanding of an object so you can quickly and effectively determine if you are interested in this object or if it is not interesting and you can move on. As part of this we feature the following tabs:

- Summary: Contains high level information about the event counts for each of tracked attributes (Domains, Samples, SID Matches, and IDS Events) as well as:
- ASN Data
- IDS Events: Events that were triggered by this IP
- GeoLocation Map: Shows where the IP is hosted.
- Domains: Contains information about any domains mapped to this IP address
- Samples: Contains a list of any samples which have been observed from this IP address.

If no information exists for the IP address searched, the user will see "No data found" in place of the respective data tab.



Figure 7: ET Intelligence Portal

#### **Current Reputation Score:**

An element is given a "confidence score" within each category. This score is not a quantitative assignment of risk, but rather reflects the degree of confidence that Emerging Threats has that the IP Address is exhibiting the behavior associated with that category. Categories include negative, neutral, and positive behaviors, and are designed for cross-correlation and context.

An IP address will often exist in multiple categories. Clicking on the Category name will toggle that category on the graph. Note that this is the current reputation score. Some categories will show as 0, regardless of the timerange selector as this is only a current not historical score like what is displayed on the graph.

✓	Category	łt	Score 🚛	First Seen	łt	Last Seen	li
✓	CnC		127	2010-09-10		2015-09-08	
<b>√</b>	ChatServer		127	2010-09-10		2015-09-08	
✓	Blackhole		120	1899-12-31		2015-09-08	
<b>√</b>	EXE_Source		0	2012-07-08		2012-11-22	
✓	Spam		0	2010-12-23		2012-04-01	

Figure 8: Current Reputation Score Table

#### **Associated Domains**

The "Domains" tab provides the user with domains that have been observed resolving to the searched IP address during that IP addresses history within the Emerging Threats system. It is important to understand that this data tab is not a WHOIS or passive DNS lookup. There may be more domains associated with an IP than display, but here Emerging Threats is presenting ONLY those domains that have been observed in the DNS process. This table also allows you to search sort based on first/last seen information, or to click on any domain to drill down.

					7 days 30 days 90 days 1 year Ma
urrent Reputation				Rep	utation History
Category	If Score L	First Seen	If Last Seen	1	io
ChatServer	78	2012-02-13	2015-09-08		
🖌 📕 CnC	0	2012-02-13	2015-08-12	1	**************************************
P2P	0	2012-07-10	2012-08-02		
Sparm	0	2012-02-13	2012-04-03	÷ Ch	0 0 0 0 0 0 0 0 0 0 0 0 0 0
ummary Domains Showing Max Domain	Samples			Last Seen	99 Mapped Domains
ummary Domains Showing Max Domain ire.zief.pl	Samples			Last Seen 2014-04-17	99 Mapped Domains 15 2012 42-14
Domains Howing Max Domain ire zief, pl mm.kepa.at	Samples			Last Seen 2014-04-17 2015-03-27	90 Mapped Domains 17 First Seen 17 2012 d0314 2013 d0316 2013 d0316
Domains stowing Max Domain ire zief.pl mm.keps.at j.kenter.pl	Samples	Ì		Last Seen 2014-04-17 2015-03-27 2015-02-28	89 Mapped Domains 10 First Seen 11 2012-00-14 2013-01-16 2012-03-18
Domains showing Max Domain ins sief, pl mm, kepa, at j, konter, pl proxim, ingalaxy; pl	Samples			Last Seen 2014-04-17 2013-03-27 2013-02-28 2013-02-28	19 Mapped Domains 2012 00:14 2013 00:14 2013 00:14 2012 00:14 2012 00:214 2012 00:214 201
Domains Rowing Max Domain In alief.pl in alief.pl in mil.kaga, at j.konter.pl proxim.ingalaxy.pl hay.rulm.ru	Samples			Last Seen 2014-04-17 2013-03-27 2013-02-28 2013-02-28 2013-02-22	Init Seen         If           2013-02-14         II           2013-02-14         III           2012-02-18         III           2012-02-18         III           2012-02-18         IIII           2012-02-18         IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII
Domains biouing Max Domain Incuist pl incuist pl incuist pl incuist pl incuist pl incuist pl incuist pl incuist pl	Samples			Last Seen           2014-04-17           2013-03-27           2013-02-28           2013-02-28           2013-02-22           2013-02-18	Pist Seen         II           2012-02-14         2012-03-16           2012-03-16         2012-03-16           2012-03-16         2012-03-16           2012-03-16         2012-03-16           2012-03-16         2012-03-16           2012-03-16         2012-03-16           2012-03-16         2012-03-16           2012-03-16         2012-03-16
Domains biouing Max Domain reclief.pl inection.pl jkonter.pl portm.iregaloxy.pl hay.rulm.ru sys.tief.pl uo.tymia.pl	Samples			Last Seen           2014-04-17           2013-03-07           2015-02-08           2013-02-08           2013-02-08           2013-02-18           2013-02-18	It         Trist Scen         It           2013-02-14         2013-02-14         2013-02-16           2012-03-18         2012-03-18         2012-03-18           2012-03-18         2012-03-08         2012-03-08           2012-02-08         2012-02-08         2012-03-08           2012-02-08         2012-03-12         2012-03-12
Domains bearing law Domain Incaled pl Incaled pl Incale	Samples			Last Seen 2014-04-17 2013-03-27 2013-02-28 2013-02-28 2013-02-28 2013-02-28 2013-02-18 2013-02-18	Ites         Ites         Ite           Ites         Ites         Ites         Ites

Figure 9: Associated domains

#### **Related Samples**

Related samples Emerging Threats has collected over the last several years. The related samples are samples which are tied to the objects being viewed. For instance, if a malicious MD5 was tracked to a given IP because a download was seen being served from that IP. The samples table includes the ability to do sorting on each column, and features information about when the sample was first seen, last seen, and what the current Virus Total Detection Ratio is for that sample. You can click on the Virus Total Detection Ratio to go to the Virus Total site for more information.



Figure 10: Related Samples

#### **IDS Events**

ETPro and ETOpen IDS Events which were triggered in the wild, and sent to the global ET SensorNet. The table features not only the signatures and a link to the signature for more information, but also information about the category for the signature, the hit count for the time period selected, and the direction the attack was detected.

14.112.3	255.81				7 days 30 days	90 days 1 yea
ASN: 133398 Registered: Owner: Tele	N/A Asia Limited	ASN Authorizer: N/A Country: N/A Reverse: N/A		SOUTHANERCA	Unite:	DopenDirectilag & Carto
DS Events Howing Max					15	Signature Events fo
Last Seen	[ SID	11 Signature		11 Src/Dst	If Categories	If Count
2015-07-21	2004662	ETPRO TROJAN IRC Bot Get http Comma	nd off-ports	Source	ChatServer	23854
2015-07-21	2808859	ETPRO TROJAN W32/Scribble-B CnC via	RC	Destination	CnC	6063
2015-07-21	2804785	ETPRO TROJAN Likely Bot User Joining IP	ic 🛛	Destination	CnC	20739
2015-07-20	2808948	ETPRO TROJAN Backdoor.Win32/Rbot IR	LOGIN	Destination	CnC	1813
2014-04-17	2000345	ET TROJAN IRC Nick change on non-stand	lard port	Destination	ChatServer	23908
2012-11-07	2017321	ET CURRENT_EVENTS SUSPICIOUS IRC XP/7	- NICK and Possible Windows	Destination	CnC	8
2012-10-31	2000348	ET TROJAN IRC Channel JOIN on non-sta	ndard port	Destination	ChatServer	19018
2012-10-31	2404100	ET CNC Spysye Tracker Reported CnC Se	rver group 1	Destination	CnC	15930
2012-10-31	2404101	ET CNC Spyeye Tracker Reported CnC Se	rver group 2	Destination	CnC	20825
2012-10-31	2003603	ET TROJAN W32. Virut A joining an IRC Ch	annel	Destination	CnC	14087
2012-10-27	2905158	ETPRO TROJAN Harrweg.gen1/Worm.AMC	0 Checkin	Destination	CnC	1
2012-07-21	2000334	ET P2P BitTorrent peer sync		Destination	P2P	11
2012-07-10	2101631	GPL CHAT AIM login		Destination	ChatServer	1
2012-04-15	2904690	ETPRO TROJAN W32 Virut CF CnC traffic		Source	CnC	28
		ET DEOR Farmhaux DEOR Listed Tertile	abarrad annual t	C	Seam	1104

#### Figure 11: IDS Samples

# **Domain Search**

Similar to the IP Address search, ET Intelligence Query allows the user to search for fully qualified domain names as well as domain plus or surrounded by the star \* wildcard (i.e. \*mydomain\*). If the domain exists, WHOIS information will be returned. If the domain searched is one of the millions contained in the Emerging Threats system of worldwide collection and malware analysis it will be returned.

The information is represented in a tabbed layout to help provide at a glance understanding of an object so you can quickly and effectively determine if you are interested in this object or if it is not interesting and you can move on. As part of this we feature the following tabs:

- Summary: Contains high level information about the event counts for each of tracked attributes (Domains, Samples, SID Matches, and IDS Events) as well as:
  - Registrar/Registrant: Who registered the domain and with whom?
  - IDS Events: Events that were triggered by this IP
  - GeoLocation Map: Shows where the IP is hosted.

- IP: Contains information about any IPs mapped to this domain
- Samples: Contains a list of any samples which have been observed from this domain
- Nameserver: Who is the authorative nameserver for this domain



Figure 12: Domain Search Results

#### **Domain Reputation History**

Domain Reputation History provides the user with the elements' categorical history within the Emerging Threats ET Intelligence Reputation system. The product of worldwide sensor placement, and massive malware sample collection and analysis, ET Intelligence Reputation assigns an element with one of 40 categories, and a score within that category. See Appendix A for a list and description of ET Intelligence Rep list categories.

An element is given a "confidence score" within each category. This score is not a quantitative assignment of risk, but rather reflects the degree of confidence that Emerging Threats has that the domain is exhibiting the behavior associated with that category. Categories include negative, neutral, and positive behaviors, and are designed for cross-correlation and context.

A domain will often exist in multiple categories. Clicking on the Category name will toggle that category on the graph at the left.

#### Associated IPs

The "IPs" tab provides the user with IP addresses that have been observed resolving to the searched domain during that domains history within the Emerging Threats system. It is important to understand that this data tab is not a WHOIS or passive DNS lookup. There may be more IPs associated with a domain than displayed, but here Emerging Threats is presenting ONLY those IPs that have been observed in the DNS process.

As with the IP address search, domain search provides the story behind the domain, and the evidence supporting its inclusion within an ET Intelligence Reputation list. Unlike the list, ET Intelligence Query will serve up domains that have been within the reputation system for up to four years, and not just those domains producing active scores that day. With access to this type of data, a user can investigate incidents that may have happened months in the past, as well as anticipate actions by actors well into the future.

The goal is to provide full context: who, what, where, when, why and how. Registrar, Registrant, and Nameservers help provide information about who. Unlike an IP address, a domain typically represents a single actor, as opposed to a shared environment. The registrant information can help a user cluster other domains by this actor and possibly relate them to known actions or intentions. An actor's calling card is often their Nameservers, and while the domains they register may be many, they often point them to the same Nameservers under their control.

The combination of Domain Reputation History and IP IDS events helps close the loop for the what, when, why and how. Categories are behaviors directly related to IDS events. Think of a category like a summary of a unique selection of alerts chosen by Emerging Threats. The categories provide a summary and level of activity score, while the IDS events are the details. Accurate ETPro rules help the user see actions, intentions and the types of tools and exploits in use. And by using timestamp tools, ETPro can determine when the methods were used.

Each tile of information within domain search presents the user with ways to relate other IOCs together. Samples can be related to domains and then the actor in the registrant detail. URLs can more uniquely identify malicious methods, while domain geolocation can present the user with an actors worldwide operational model.

With the full story, investigations can end quicker, IOCs can be shared and actions can be prioritized.

urrent Reputation				Reputation History
Category	If Soore LE	First Seen	# Last Seen #	
🗹 🚦 Blackhole	124	2013-01-17	2015-09-08	
ChatServer	124	2011-08-03	2015-09-08	
🖉 📱 CHC	112	2010-12-02	2015-09-08	
EXE_Source	0	2012-07-02	2012-11-22	
				Sali 2011 Sali 2012 Sali 2015 Sali 2014 Sali 2015
immary IPs Sa howing Max	amples Names	servers		Blackhols Chutterver CiriC EXE_Source Source
ummary IPs St howing Max IP Address	amples Names	servers	11 Lasi Seco	Blackhols Chutterver CiriC EXE_Source Souri 38 Resolved IP
ummary IPs St howing Max IP Address 24 248 155 155	amples Names	servers	11 Last Seen 2015-02-07	Blackhols Chutterver CiriC EXE_Source Souri 38 Resolver (P 1) First Seen 2014-05-02
Immary IPs Sa howing Max IP Address 24 248 156 166 87 215 05 149	amples Names	servers	11 Last Sen 2015-02-07 2015-01-18	Blackhols Chutterver CiriC EXE_Source Souri 38 Resolver (19 19 19 19 19 19 19 19 19 19 19 19 19 1
IT Address 24 248 155 155 27 215 05 149 226.149.30 57	amples Names	servers	11 Last Seen 2015-02-07 2015-01-18 2014-12-22	Blackhols Chutterver CiriC EXE_Source Souri 38 Resolver (P 2014-05-02 2014-05-02 2014-05-02 2014-05-02
ummany IPs St houing Max IP Address 24 246 135 155 67 215 65,149 216,149,35 57 24 249 52,54	amples Namee	servers	It         Last Seen           2015-02-07         2015-01-18           2014-12-22         2014-12-22	Biskhols         Chatterver         Circl         EXE_Source         Span           38 Resolved (P           19         First Seec         2014-052           2014-0428         2014-0428         2014-0428           2014-0428         2014-0428         2014-0428
umman) IPs St houing Max IP Address 24 246 135 155 57 215 05 149 216, 149 32 54 24 249 32 54 148, 51 111, 111	amples Namee	servers	11 Last Seen 2015-02-07 2015-01-18 2014-12-22 2014-12-22 2014-05-12	Biskhols         Chatterier         Circl         ERE_Source         Span           38 Resolved (P           19         First Szec         2014-05-02           2014-05-02         2014-04-03         2014-01-02           2014-01-02         2014-01-02         2014-01-02
ummary IPs St houling libas IP Address 24 246 155, 155 57 215, 05, 149 210, 140, 30, 57 24 240 152, 34 142, 81, 111, 111 64 237, 22, 230	amples Names	servens	III         Last Seen           2015-00-71         2015-01-18           2014-01-22         2014-01-22           2014-01-22         2014-00-12           2014-00-12         2014-00-12	Biskhols         Chatterier         Circ         ERE_Source         Span           38 lineatured (P           1         First Seen         2014/0-00           2014/0-00         2014/0-00         2014/0-00           2014/0-02         2014/0-02         2014/0-02           2014/0-02         2014/0-02         2014/0-02           2014/0-02         2014/0-02         2014/0-02           2014/0-02         2014/0-02         2014/0-02
Inmany IPs St houng Max IP Address 24 248 156 165 27 275 05 149 216,146,36 37 212 269 234 148,85 351,159 24 249 25,220 24 249 24,159	amples   Names	servers	III         Last Seen           2015-02-07         2015-01-16           2015-01-16         2014-12-22           2014-12-22         2014-12-22           2014-08-04         2014-08-04           2014-08-06         2014-08-06           2014-08-06         2014-08-06	Biskhols         Chatterer         Circ         EXE_Source         Span           38 Resolved (P)         Size         Size <t< td=""></t<>

Figure 13: Associated IP Addresses

#### Nameservers

The servers that respond with the IP address of the domain in question. Note that this can change over time. In Figure 16, the nameserver has been changed to a sinkhole as the domain has been condemned.

Cur	rent Reputation					Reputation History
1	Category J	lt Score LE	First Seen	ш	Last Seen 1	
1	Blackhole	124	2013-01-17		2015-09-08	120
1	ChatServer	124	2011-03-03		2015-09-08	
1	Circ	112	2010-12-02		2015-09-08	°
	EXE_Source	0	2012-07-02		2012-11-22	
1	Spam	٥	2010-12-01		2012-03-27	
Shor	mary Pa San	noles Name	servers			Jan 2011 Jan 2012 Jan 2018 Jan 2014 Jan 2015 Blackhole Challerver Cric ERE_Source Span 1 Namaservers face
N	ame Server				Last See	First Seen II

Figure 14: Associated Nameservers

#### **Related Samples**

Related samples Emerging Threats has collected years of threat samples which contain an instance of the searched domain within the network traffic captured by Emerging Threats when the sample was executed on a virtual host. Clicking on a hyperlinked sample will produce a sample search, and take the user to the Sample Analysis page.

urrent Reputation					Reputation	History					
Category	If Score	First Seen	11 Last Seen	н	140					in the second	
Blackhole	124	2013-01-17	2015-09-08		120	1801	THANK		N N	114	ų,
ChatServer	124	2011-03-03	2015-09-08		100				A A		ľ
🗸 📕 снс	112	2010-12-02	2015-09-08		80				11/1	7	
EIE_Source	0	2012-07-02	2012-11-22		00					11	
Spam	0	2010-12-01	2012-03-27		+0						
					- 14						
					Jan 2011	Jan I	2012 Jan 201	13 Jan	2014	Jan 2015	
_	-										
Summary IPs S Showing Max	amples	lameservers							5,000	Samples (	coller
Showing Nax	amples	lameservers		H L	ist Seen	1ž	First Seen	8	1,000 VirusTotal Rabio	Samples ( Detection	collect
ummary IPs S showing Max NOS 02017aa1705ado1d5df2	amples N	lameservens		<b>#</b> 10 20	est Seen 115-08-07	ŧ	First Seen 2015-09-07	11	1,000 VirusTotal Ratio 43/00	Samples ( Detection	toller
NDS	amples N 963c812r5rrr 41c8850eb4f7	lameservens		<b>41</b> 12 22 23	est Seen 115-09-07 115-09-07	17	First Seen 2015-08-07 2015-09-07	Ħ	1,000 VirusTotal Rabio 43/03 45/57	Samples C	Coller
Ummary IF8 S Sewing Nax NDS 02077aa1705ade1e5612 027e7044ea5014ca800F 02548acod53856905e80	amples N 863691215111 41cb880eb447 86567aaa1476	lameservens		H 12 22 23 23	115 Seen 115-09-07 115-09-07	ţ	First Seen 2015-09-07 2015-09-07 2015-09-07	Ħ	1,000 VirusTotal Rabio 43/05 45/67 45/67	Samples ( Detection	collec
Ummary IPs S Rowng Nax MOS 00717aa1705aste1e5042 00747448ace643265950600 00168ac120448ac9645647	amples 8 863x91215fff 4fcb880eb4f7 65b6fsex1475 276172827#40	lameservera		44 L 22 23 23 24 24 24	est Seen 115-09-07 115-09-07 115-09-07	ŝ	First Seen 2015-09-07 2015-09-07 2015-09-07 2015-09-07 2015-09-07	H	1,000 VirusTotal Ratio 43/00 45/07 45/07 45/07	Samples (	Collec
Ummary IPe S Proving Max MDS 002171aa1705ab01405421 002429acods265005400 001ables12244850545427 0023623402425652445	amples N 883x612/5/rrr 4/5x880x64477 85507aac1476 275872827x48	lameservers		11 13 22 23 23 24 24 24 25 25 25 25 25 25 25 25 25 25 25 25 25	nt Seen 115-09-07 115-09-07 115-09-07 115-09-07	Ĩ	First Seen 2015-09-07 2015-09-07 2015-09-07 2015-09-07 2015-09-07 2015-09-07	Ħ	1,000 VirusTotal Ratio 43/00 45/67 48/67 48/67	Samples (	Collec
Ummary IPe S Proving Max NOS 002171a117054501405012 00247940645021665056050 001stille=120455627 002262240245824564547	amples N 8636812/5/17 41686069477 868619661470 278172827#49 778574539170 1/168394051576	ameservers		41 22 22 23 23 23 24 24 24 25 25 25 25 25 25 25 25 25 25 25 25 25	nt Seen 15-08-07 15-08-07 15-08-07 15-08-07 15-08-07 15-08-07	žt	First Seen 2015-08-07 2015-08-07 2015-08-07 2015-08-07 2015-08-07 2015-08-07	Ħ	1,809 Virus1otal 43/00 45/07 48/07 48/07 48/07 48/07	Samples ( Detection	Collec
Ummary IPs S aboverg Max NOS 000773a1705464105142 0074644001464064 00106404050546400 001064140405054640 01272601563160386200 0186264540405077150	8036912/55/77 4166950664477 05057aac1470 05057aac1470 7780545391570 142839405157c 142839405157c	ameservers		41 22 23 23 23 24 24 24 24 24 24 24 24 24 24 24 24 24	nt Seen 115-08-07 115-08-07 115-08-07 115-08-07 115-08-07 115-08-07	ŝ	First Seen 2015-09-07 2015-09-07 2015-09-07 2015-09-07 2015-09-07 2015-09-07	ł	1,609 VirusTotal 43/00 45/67 48/67 48/67 48/67 48/67	Samples (	
Ummary IPs S Rowing Max MOS 00077au1703u6145072 00724045x400146467 00026238630408660 01168641634046677155 01006001674517306150	803e912/55/77 41cb808eb467 00505face1470 278672427+49 773624839475 14285425f5f5 44276565742b	ameservers		41 22 22 23 23 24 24 24 25 25 25 25 25 25 25 25 25 25 25 25 25	est Seen 15-08-07 15-08-07 15-08-07 15-08-07 15-08-07 15-08-07 15-08-07 15-08-07	Ţ	First Seen 2015-09-07 2015-09-07 2015-09-07 2015-09-07 2015-09-07 2015-09-07 2015-09-07	11	1,800 VirusTotal A300 4507 4507 4807 4807 4807 4807 4807 4807 4807 48	Samples (	Collec

Figure 15: Related Samples

#### **IP IDS Events**

I

ETPro and ETOpen IDS Events fired by the IP address that the searched domain resolved to during the Sandnet execution process. Here the IP that fired the alert will be a destination IP address. The hyper link to the left is the Emerging Threats SID (signature identifier), and can be clicked to take the user to a SID search. The signature column presents the user with the MSG field of the actual rule.

nain: ilo	.brenz.p				7 days	30 days	90 days	a 1 year
DS Events Showing Max						47	Signature	Events four
Last Seen	17 SID	IT Signature	H Sr	to/Dst		Categories		Count II
2015-09-05	2019354	ET TROJAN Reply Sinkhole - irc-sinkhole cert.pl	So	urce	1	Blackhole		57792
2015-09-05	2000345	ET TROJAN IRC Nick change on non-standard port	De	estination		ChatServer		1084
2015-09-05	2000859	ETPRO TROJAN W32/Scribble-B CnC via IRC	De	estination	2	⊃nC		5023
2015-09-05	2804785	ETPRO TROJAN Likely Bot User Joining IRC	De	stination	1	Diric		1080
2015-08-27	2906946	ETPRO TROJAN Backdoor. Wh32/Rbot IRC LOGIN	De	stination	1	SnC		90
2015-08-27	2009603	ET TROJAN W32 Virut A joining an IRC Channel	De	stination		CnC		103
2015-00-29	2000348	ET TROJAN IRC Channel JOIN on non-standard port	De	stination		ChatServer		17
2014-12-14	2811079	ETPRO TROJAN Win32/Virut.BN Dropper HTTP Request	De	estination	4	OnC		376
2014-09-12	2017001	ET TROJAN Connection to a cert.pl Sinkhole IP (Possible Infected Host)	D	estination		Blackhole		14248
2012-10-23	2404101	ET CNC Spyleye Tracker Reported CnC Server group 2	De	stination	9	OnC		4612
2012-10-07	2404100	ET CNC Spyeye Tracker Reported CnC Server group 1	De	estination		DnC		4494
2012-09-20	2804682	ETPRO TROJAN IRC Bot Get http Command off-ports	So	urce .		ChatServer		14
2012-09-28	2903276	ETPRO TROJAN Win32/Ramat: A PING INBOUND	Se	urse		OnC		72
2012-08-24	2404110	ET CNC Spywyw Tracker Reported CnC Server group 11	D,	estination		DnC		2115
2012-09-20	2000419	ET POLICY PE EXE or DLL Windows file download	So	urce		EXE_Bource		188
2012-09-20	10000029	FILE ET magic PE32	Se	urce		EXE_Source		185
2012-08-20	2007671	ET POLICY Binary Download Smaller than 1 MB Likely Hostile	Se	urce	1	EXE_Source		182
2012-09-18	2404109	ET CNC Spyeye Tracker Reported CnC Server group 10	De	estination		SnC		773
2012-08-07	2014819	ET INFO Packed Executable Download	Se	urce	1	EXE_Source		1
2012-09-07	2015744	ET INFO EXE (sDebuggerPresent (Used in Malware Anti-Debugging)	So	urce	1	EXE_Source		1
2012-08-09	2026.077	ETDRO TROJAN W32 Vind CE ava request	De	etiention		Cerci i		31

Figure 16: IDS Events

The network doesn't lie. Today, advanced malware can evade endpoint antivirus. The ET Intelligence Query Sample Search feature was designed to present the user with an unbiased and untainted view of malware in motion—from a perspective that is harder to tamper with.

The sample analysis page provides the user with the same type of information that our world-class research team uses to write the ETPro ruleset. The user is presented with four different perspectives on network traffic. Each perspective arms the user with a chance to catch anomalies that might not be detected by the prior tab.

Even in situations where no alerts are fired, the user is still given many options to detect, or relate to other IOCs in order to continue an investigation that had reached a dead-end.

#### Sample Search

ET Intelligence Query allows the user to search based upon the MD5 hash of a sample in the Emerging Threats sample database. Emerging Threats possesses hundreds of millions of samples that include DLL files, PDFs, EXE files, MS Office documents and much more.

A sample search will take the user to the Sample Analysis page. The sample analysis page includes metadata about the sample, and a tabbed index of the network traffic that sample produced when executed on a host including the TCP/IP, DNS, and HTTP connections. A link to Virus Total using the searched sample is also provided at the bottom of the sample metadata field.

#### Sample: 757782d6a88684b923aabbba62157205

IDS 757782d6; Jubmision Dat ype PE32 exer	488084b923aabb e 2015-01-03 0 outable for MS V	ba02:107205 55 0:22:37 Fi Vindows (GUI) Intel 80386 32-bit Vi	4A256 040bc5452ca le Size 209408 rusTotal 14/58	407103202	2ca4b1a602f3ab8	fdoo631963b0156	07db028db8077ae	
lerts Cor	nnections	DNS HTTP						
Date 📙	Sid 1	Signature	ų	Rev II	SrcIP 🛔	SrePort 💵	DstiP	DstPort #
2015-01-03	2019138	ET TROJAN Win32/Poweliks GET Request		3	private	1038	31,184,192,80	80
2015-01-03	2014620	ET INFO EXE - Served Attached HTTP		6	23.16.5.213	80	private	1037
2016-01-03	2808248	ETPRO TROJAN Win32/Poweliks A Checkin		2	private	1035	31.184.192.80	80
2015-01-03	2808248	ETPRO TROJAN Win32/Powelike A Checkin		2	private	1036	31.184.192.80	80
2015-01-03	10000029	FILE ET magic PE32		2	23.15.5.213	80	private	1037
2015-01-03	2000419	ET POLICY PE EXE or DLL Windows file downloa	be	22	23.15.5.213	80	private	1037
	TONTERS :	ET DOLINY are doubled up LITTR - Information	al land		ariunta.	1027	22.15.6.212	80

#### Figure 17: Sample Analysis Page

There are occasions where ET receives PCAP files that detail the network traffic of certain threats. In those situations, the sample analysis page will still index that traffic using the four tabs described below, the only difference is that the MD5 sum is that of the PCAP file and not the sample. Type, SHA256, and file size will be marked "NA." An example of this condition is below:

Sample Analysis Tabs include:

- Alerts
- Connections
- DNS
- HTTP

SID search offers perhaps the most powerful and compelling feature of the tool. ETPro signatures are the primary method in which ET as an organization, expresses itself. So if you were to ask ET, "What is this particular Exploit Kit doing these days," the response would be a collection of signature identifiers (SIDs). We could tell you what the landing page looked like, what redirection method they used, how they exploited java and what actions after compromise looked like—all using ETPro SIDs.

With this in mind the user is able to take SIDs from their alert console and get a global perspective on something that happened locally. Using SID search, the user could see related IOCs, actions, tools, and help piece together the intrusion kill chain that surrounds a single event they maybe looking at in a console.

Here the user is able to see the entire body of an attack before it happens so that they can align their defenses accordingly, or piece together an intrusion that already took place using the context provided by ET Intelligence Query.

#### **Tab descriptions**

#### Alerts

The Alerts tab displays the ETPro and ETOpen IDS Alerts that were fired while observing network traffic to and from the host during sample execution. Samples have unrestricted access to the internet during execution. All columns on the alerts tab can be sorted from high to low or low to high. Hyperlinked IP addresses can be clicked to arrive at an IP address Search. The search function of this tab will search rule MSG body and other fields.

#### Connections

The connections tab presents a list of connections made by the host that the sample was executed on. All columns on the connections tab can be sorted from high to low or low to high. Hyperlinked IP addresses can be clicked to arrive at an IP address Search.

#### DNS

The DNS tab presents a list of DNS transactions from the host that executed the sample in question. All columns on the connections tab can be sorted from high to low or low to high. Hyperlinked IP addresses and domains can be clicked to arrive at an IP address Search.

#### HTTP

The HTTP tab presents a list of the extracted HTTP headers based upon HTTP transactions performed by the host that executed the sample. All columns on the connections tab can be sorted from high to low or low to high. Hyperlinked IP addresses and domains can be clicked to arrive at an IP address Search.

# **SID Search**

ET Intelligence Query allows a user to search based upon the ETPro or ETOpen Signature ID number. This search will return the associated IP addresses that have been seen fired the alert in question around the world and in the Emerging Threats proprietary Sandnet. IP addresses can be sorted to produce a sequential list.

. 2004002		7 daya 30 daya 90 daya 1 year
Compromised Workstation	ETPRO TROJAN IRC Bot Get h	ttp Command off-ports
This alort is triggered when traffic A Trojan Checkin event occurs when a oredit card numbers, and login oreden	nothing a known Command and Control pattern is observed. a compromised host contacts a command and control server. A Chied dats which could be sent to the attacker, and commands will often be	kin may contain gathered personal or computer information, banking details. Instande to the infected system.
Rule Text Surioata Text		
alert tep SEXTERNAL_MET (6000) G"; content:"get[20]http[3s 2f	2000 -> SHONE_NET any (mmg: "ETPRO TROIGN ENC Bot Get http: 27 "; distance:0; reference:nd5,93c57fee5a482a776fe6ddfc6	Command off-ports"; flow.established,from_server; content "PRDM" LaSSelb7; classrype:trojan-activity; cid:2304682; rev:1;)
Smort Tent		
<pre>slort top SECTEDNAL_NET 10000: 0"; content:"get[20]http[3s lf</pre>	NODE → SHORE_RET any (mag:"ETHID INCIAN DRC Bot Get Http 27 "; dLatance:0; reference:nd5,03c57fee3e482d7f5fe6ddfc6	Command off ports"; flow:coteblished,from_server; content:"PNDV9 We55elb7; classtype:trojan-activity; sid:2004882; rev:1;)
estination IPs Source Ps	Domans Samples References	
And a state of the		
Showing 1 year		11 Related Destination IPS for
Bhowing 1 year	II Last Seen	11 Related Destination IPS fo
Bhoving 1 year Relidress Bh 38 123 137	17 Last Seen 2014-12-01	11 Related Destination IPG for 2014-11-23
Bhowing 1 year Bh Address Bh 38 133 137 126 40 34.1	If         Last Seen           2014/12:01         2014/12:01	11 Related Destroads IPD for IF Fired Seen 2014-11-23 2014-11-10
Proving 1 year P Address 80 26 122 127 128 40 34.1 88.38 201.81	Inst Seen           2014-12-01           2014-12-01           2014-11-01           2014-11-17	11 Related Destroader IPG for 2014-11-23 2014-11-10 2014-11-10
Address     A	1 stati Soon           2014-12-201           2014-12-201           2014-1417           2014-141-127	11 Related Destruction IPD for 2014-11-23 2014-11-10 2014-11-10 2014-11-10 2014-11-02
Proving 1 year     Posta     Po	Itati Even           2014-12-201           2014-12-201           2014-14-107           2014-14-102           2014-11-22	11 Robert Destroads IPS to 11 Robert Destroads IPS to 2014-11-23 2014-11-29 2014-11-40 2014-11-42 2014-11-42
Proving 1 year     Paddrase     Paddras	Itati See           2014-12-201           2014-12-201           2014-12-201           2014-11-02           2014-11-02           2014-11-02           2014-11-02           2014-11-02           2014-11-02           2014-11-02	11 Robert Destroads IPS for 2014-11-23 2014-11-23 2014-11-29 2014-11-29 2014-11-29 2014-11-29 2014-11-29 2014-11-29 2014-11-29
Booling 1 year     Booling	21         1.541 Soon           2014-12-01         2014-12-01           2014-12-01         2014-11-02           2014-11-02         2014-11-02           2014-11-02         2014-11-02           2014-11-02         2014-11-02           2014-11-02         2014-11-02	11 Robert Destroades IPG for 2014-11-23 2014-11-23 2014-11-29 2014-11-29 2014-11-20 2014-11-20 2014-11-20 2014-11-20
Broing 1 year     Books 131 337     Books 131 337     Books 131 337     Books 131 337     Books 131     Hot 1314 346     Hot 1314 346     Hot 1314 346     Hot 1314 346     Hot 1314     Hot 131     Hot 1314     Hot 131     Hot 131	2141 Som           2014-12-01           2014-12-01           2014-12-01           2014-11-02           2014-11-02           2014-11-02           2014-11-03           2014-10-13           2014-00-13           2014-00-13	11 Related Destination (PD 6) 2014-01-02 2014-01-02 2014-01-02 2014-01-02 2014-01-02 2014-01-03 2014-01-03 2014-01-03
Broing 1 year     Book 1 year     Book 2 year	1 stat Som           2014-12-01           2014-12-01           2014-11-201           2014-11-201           2014-11-201           2014-11-201           2014-11-201           2014-11-201           2014-11-201           2014-11-201           2014-11-201           2014-11-201           2014-11-201           2014-11-201           2014-11-201           2014-11-201           2014-11-201           2014-11-201           2014-11-201	11 Related Destruction IPG for 2014-11-23 2014-11-23 2014-11-29 20 2014-11-29 2014-11-29 2014-11-29 2014-11-29 2014-11-29 2014-11-29

Figure 18: SID Search

SID search also produces the domains that have been observed associated with SID and IP address pairings within the Emerging Threats proprietary Sandnet. A list of associated samples is also presented that when clicked produces a Sample analysis of the MD5.

# **Search History**

In the Threat Intelligence system, we now provide a Search History capability which allows you to easily sift back through any searches which you, or anyone in your organization have done in ET Intelligence. This is very helpful for working cooperatively with others as well as recalling past searches. Simply click on the Search History button at the top of the screen. You can also click on any of the search terms to be brought to the current page for that object.

User email 🛛 👫	Type II	Term 11	Date	1
bwoodberg@proofpoint.com	multidom	raiel."	2015-09-08 22:51:09	
bwoodberg@proofpoint.com	domain	in sid p	2015-09-08 22:47:01	
bwoodberg@proofpoint.com	φ	114.112.200.81	2015-09-08 22:27:37	
bwoodberg@proofpoint.com	sample	75778200x88084b923xx1bbx02157205	2015-09-08 22:24:19	
bwoodberg@proofpoint.com	sid	2804582	2015-09-08 22:22:29	
bwoodberg@proofpoint.com	domain	ib brenz pl	2015-09-08 22:22:00	
bwoodberg@proofpoint.com	iρ	114.112.205.81	2015-09-08 22:21:27	
bwoodberg@proofpoint.com	sid	2904682	2015-09-08 20:45:25	
bwoodberg@proofpoint.com	sample	757782d0x608084b923xxbbbx82157205	2015-09-08 20:39:54	
bwoodberg@proofpoint.com	domain	ilo.txenz.pl	2015-09-08 20:31:54	
bwoodberg@proofpoint.com	ф.	114 112 255 81	2015-09-08 20:18:15	
buroodberg@proofpoint.com	io	50 20 10 5	2015-09-08	

Figure 19: Search History

# **Appendix A**

#### **Categorization legend**

Each ET Intelligence Rep List entry is given one of the following categories, and is displayed in the list with its corresponding category number:

- 1, CnC, Malware Command and Control Server
- 2, Bot, Known Infected Bot
- 3, Spam, Known Spam Source
- 4, Drop, Drop site for logs or stolen credentials
- 5, SpywareCnC, Spyware Reporting Server
- 6, OnlineGaming, Questionable Gaming Site
- 7, DriveBySrc, Driveby Source
- 9, ChatServer, POLICY Chat Server
- 10, TorNode, POLICY Tor Node
- 13, Compromised, Known compromised or Host
- 15, P2P, P2P Node
- 16, Proxy, Proxy Host
- 17, IPCheck, IP Check Services
- 19, Utility, Known Good Public Utility
- 20, DDoSTarget, Target of a DDoS
- 21, Scanner, Host Performing Scanning
- 23, Brute\_Forcer, SSH or other brute forcer
- 24, FakeAV, Fake AV and AS Products
- 25, DynDNS, Domain or IP Related to a Dynamic DNS Entry or Request
- 26, Undesirable, Undesirable but not illegal
- 27, AbusedTLD, Abused or free TLD Related
- 28, SelfSignedSSL, Self Signed SSL or other suspicious encryption
- 29, Blackhole, Blackhole or Sinkhole systems
- 30, RemoteAccessService, GoToMyPC and similar remote access services
- 31, P2PCnC, Distributed CnC Nodes
- 32, SharedHosting, Known Shared Hosting server
- 33, Parking, Domain or SEO Parked
- 34, VPN, VPN Server
- 35, EXE\_Source, observed serving executables
- 37, Mobile\_CnC, Known CnC for Mobile specific Family
- 38, Mobile\_Spyware\_CnC, Spyware CnC specific to mobile devices
- 39, Skype\_SuperNode, Observed Skype Bootstrap or Supernode
- 40, Bitcoin\_Related, Bitcoin Mining and related
- 41, DDoSAttacker, DDoS Source

Periodically we add and retire categories from the published lists. To date, we have kept data and reputation attribution mechanisms active and associated with 40 different categories. Some categories, however, may be retired from publishing because it is more effective to globally safelist trusted sites instead of having them as a category. For others, we have removed categories that might be confusing or not relevant. In each case we may continue to track and maintain the category, but not publish it—this allows us to tweak attribution mechanisms, as well as create categories for R&D purposes.

#### Background & legend for each category:

1, CnC, Malware Command and Control Server

Observed or DGA predicted domains and IPs that are command and control for known Trojans. These listings are specifically criminal, differentiated from spyware and user tracking domains, which are classified in SpywareCnC.

#### 2, Bot, Known Infected Bot

A host observed checking in to a command and control server, or exhibiting clear indications of unwanted and criminal code on the host.

#### 3, Spam, Known Spam Source

We don't track all spam sources, but those observed sending spam or being rejected as blocklisted are included.

#### 4, Drop, Drop site for logs or stolen credentials

Differentiated from CnC servers, but sometimes overlapping. Anywhere we see stolen data or credentials being pushed. Does not include droppers being served or other exe movement.

#### 5, SpywareCnC, Spyware Reporting Server

Servers and domains observed being used to serve or track user activity. Specifically not clearly criminal, but we avoid plain adserving sites as much as is possible. Generally these are going to be toolbars, rogue gaming, free screensavers and more.

#### 6, OnlineGaming, Questionable Gaming Site

Gambling, flash games, and similar that installs a client and report or track user activity. Most of these do not cross the line of criminal, but are differentiated from plain spyware activity.

#### 7, DriveBySrc, Driveby Source

Kit redirectors, exploit serving, or injected or compromised sites that either have attempted to or will lead to a compromised browser. DriveBySrc is a category representing sites that have been utilized by various exploit kits such as Neosploit or Blackhole, where via some sort of HTML injection, a users browser is redirected to these sites that deliver an exploit by java or some other method.

#### 9, ChatServer, POLICY Chat Server

Observed chat activity, including but not limited to IRC, Jabber, Google Talk, MSN, AIM, ICQ, Baidu, GaduGadu and more. This is not an indication of hostab activity, only known chat activity. Can be cross-correlated with CnC to help mitigate legitimate IRC networks in use as CnC.

#### 10, TorNode, POLICY Tor Node

Identification of Tor exit nodes and participants seen in the network.

13, Compromised, Known compromised or Hostab A bit of a catchall category for hosts that are observed hostab including compromised web servers, brute forcers, or otherwise not easily classifiable activity.

#### 15, P2P, P2P Node

Observed clients and sources of generally legitimate file sharing, including traditional bittorrents, limewire or kazaa, qvod and others.

#### 16, Proxy, Proxy Host

Observed proxy endpoint for http, stun, socks and more.

#### 17, IPCheck, IP Check Services

IP and geo check services. Generally public services which are very often abused by malware or dyndns activity.

# 19, Utility, Known Good Public Utility

Known good nets and services such as Google search frontends, Bing and more.

#### 20, DDoSTarget, Target of a DDoS

Observed DDoS targets by traffic or observed commands to launch attacks to these nets.

#### 21, Scanner, Host Performing Scanning Web vulnerability scanning; open relay scanning, network and service recon, and often Nessus or other scanner activity.

#### 23, Brute\_Forcer, SSH or other brute forcer

All observed authentication brute forcing, including SSH, imap, VNC and more.

#### 24, FakeAV, Fake AV and AS Products

Fake antispyware and av product sites being sold or distributed. Often overlaps with CnC.

# 25, DynDNS, Domain or IP Related to a Dynamic DNS Entry or Request

Host or domain observed using DynDNS.

#### 26, Undesirable, Undesirable but not illegal

Some hack tool forums, metasploit updates and more. Not illegal, but of interest on an otherwise controlled network.

27, Abused TLD, Abused or free TLD Related Activity or DNS related to rogue TLD and GTLDs such as .tk, co.cc, and others. Not always hostab, but of interest. Reserved for rogue registrars...registrars that either can't, or choose not to police their domains, and TLDs that are free or with less accountability. The TLD .su is a perfect example. ICANN can't claim a domain back from a country (Soviet Union) that no longer exists. Malicious

activity in this category isn't certain, but typically suspicious.

28, SelfSignedSSL, Self Signed SSL or other suspicious encryption Self-signed or other invalid SSL certificates in use.

29, Blackhole, Blackhole or Sinkhole systems

Known sinkhole in use by a trusted organization. Will often overlap with CnC.

30, Remote Access Service, GoToMyPC and similar remote access services

Observed but often legitimate remote access services like Kaseya, Gotomypc, Citrix, and others.

#### 31, P2PCnC, Distributed CnC Nodes

Zeus and other families that use P2P as a CnC mechanism. Separated category to handle the volume and transient nature of these hosts.

33, Parking, Domain or SEO Parked Known parked domain or parking server.

34, VPN, VPN Server

VPN protocols observed using this address as a concentrator. Potential anonymizing service.

35, EXE\_Source, Observed serving of an Executable. Not necessarily hostab, but will often coincide with CnC.

40, Bitcoin\_Related is a category based upon observed activity related to P2P Bitcoin mining. The focus here is not a user making transactions with Bitcoins, but actual Bitcoin clients running in the Bitcoin P2P network. This can help identify the rogue use of computing resources in Bitcoin mining operations.

41, DDoS Attacker, Source of DDoS traffic.

# **LEARN MORE**

For more information, visit **proofpoint.com**.

#### ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at www.proofpoint.com.

©Proofpoint, Inc. Proofpoint is a trademark of Proofpoint, Inc. in the United States and other countries. All other trademarks contained herein are property of their respective owners. Proofpoint.com

# proofpoint.