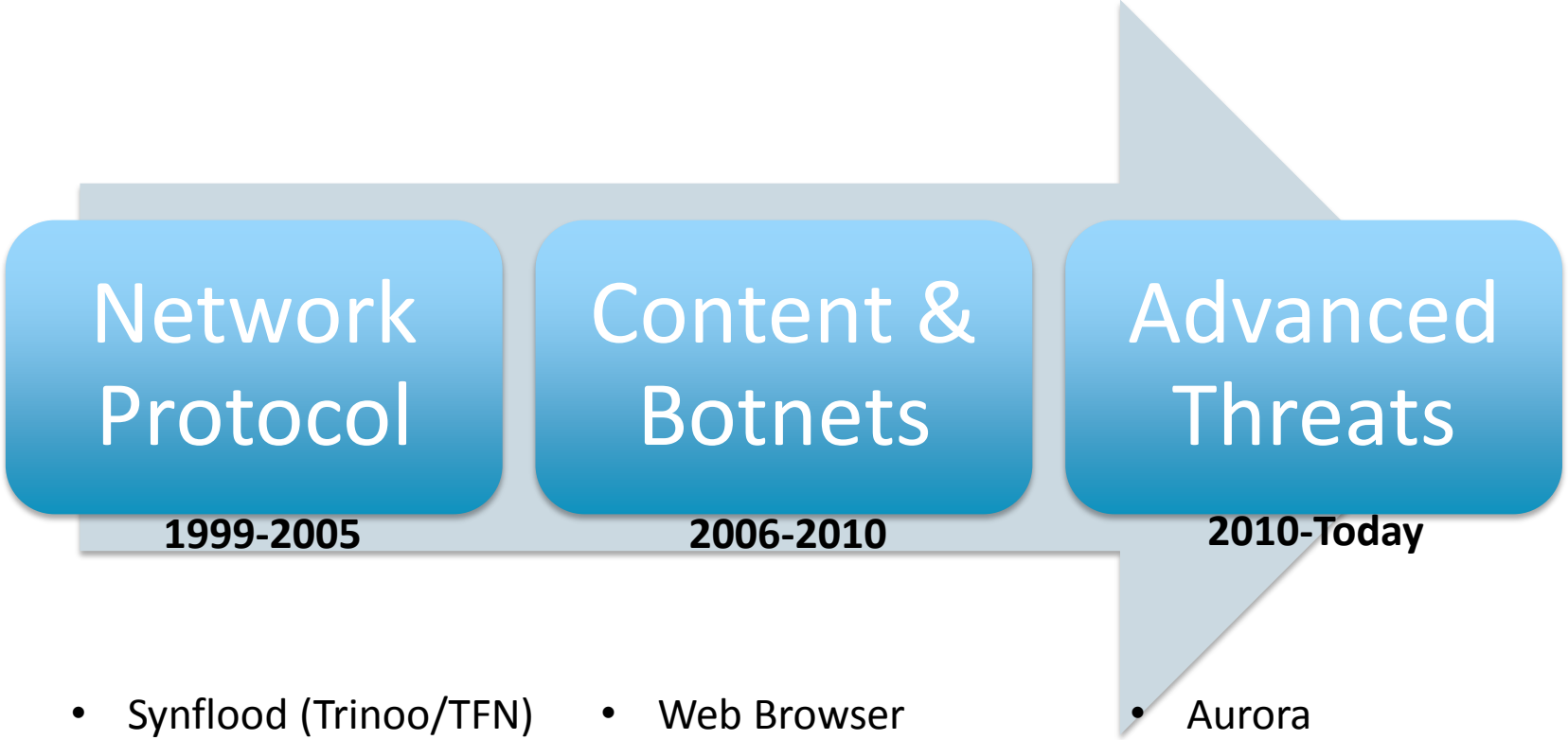
Evolving Advanced Threat Landscape

A close look at PoS Malware Attack Campaigns

Threat Landscape Era's



- Synflood (Trinoo/TFN)
- Code Red
- Slammer
- Zotob
- Conficker (2008)

- Web Browser
- Web Applications
- Doc/PDF/etc.
- Flash/Shockwave
- Java

- Aurora
- Operation Payback
- Stuxnet/Flame/Duqu
- Red October
- Cyber Warfare

ARBOR NETWORKS

What is "Advanced Threats"

An Advanced "Threat" is a series of events – a targeted campaign of attacks – that put an organization at risk.

It is…

- ✓ Inclusive of attacks, evasion techniques, diversion processes.
- ✓ Multiple types of attacks.
- ✓ Targeted at a specific organization.
- ✓ Is planned.
- ✓ Includes different stages of attack execution.

It is not…

- ≠ A single attack
- ≠ Just malware or just DDoS
- ≠ Executed by chance.
- ≠ Targeted at a general population.

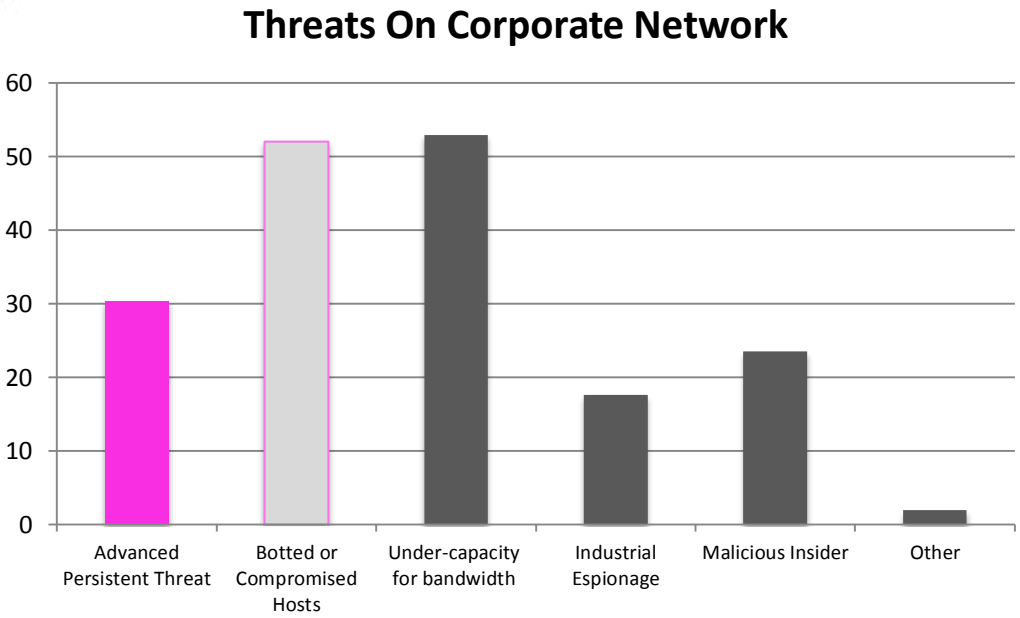
ARBOR NETWORKS

Why do Threats get Through?

- Huge number of 'ways in'
  - Drive By Download
  - SPAM/Phishing
  - Watering Hole
  - Obfuscation
  - USB

- Many Threat Vectors
  - New AND Old
  - IPS / AV Limited coverage
  - Patching lag

- Leveraging vulnerabilities in:
  - Java applets
  - Compound Documents
  - Anything Adobe

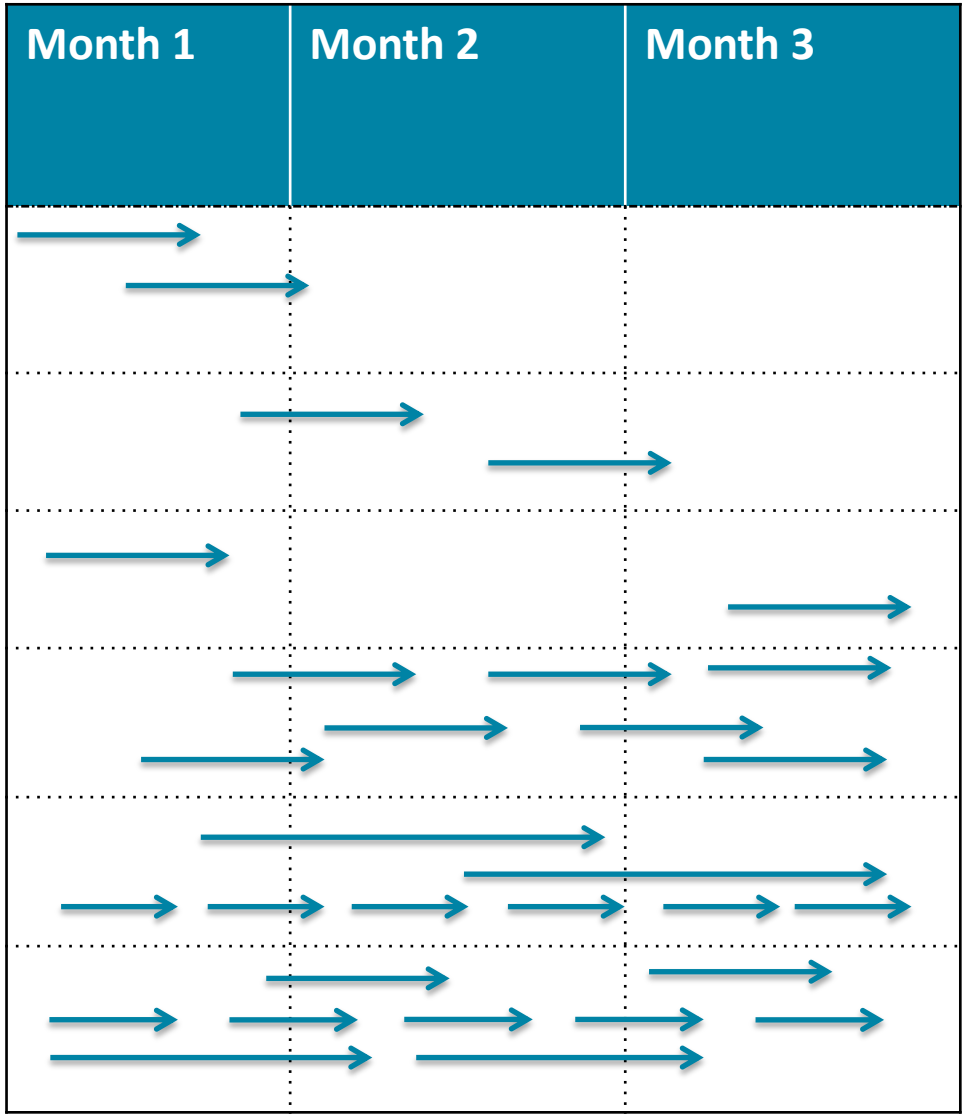


ARBOR NETWORKS

Advanced Threats - Targeted Attack Campaigns

Example Tools in Advanced Threat Campaign

- Phishing
- RAT
- DDoS
- Zero Day Exploits
- Malware
- Evasion Techniques



Most vendors are focused on stopping individual attacks – not campaigns

ARBOR NETWORKS

Happy Holidays: PoS Malware Campaign

Target hacked: news and updates on the massive retail breach that affected millions

By Chris Welch on January 16, 2014 01:42 pm Email

Between November 27th and December 15th, 2013, retail giant Target fell victim to a sophisticated hack that compromised data on tens of millions of its shoppers. Information on approximately 40 million credit and debit card accounts was stolen during the breach, and this sensitive financial data quickly appeared on the black market. Target would later reveal that names, mailing addresses, and phone numbers for up to 70 million customers had also been taken during the attack. The retailer is cooperating with the US Secret Service and Department of Justice to find those responsible; those perpetrators currently remain at large. Target's holiday breach ranks as one of the largest retail hacks in history. In response to the ordeal, the company offered affected customers one year of

ARBOR NETWORKS

PoS Malware: Big Picture

- Point of Sale machines
  - Process credit and debit cards
- Malware steals card data
  - Typically by scraping memory
  - PoS malware includes Dexter, Project Hook, Alina, vskimmer, RammScraper & Soraya (discovered on 21 May 2014)

ARBOR NETWORKS

PoS Malware: Dexter and Project Hook

- Dexter & Project Hook
  - Card data → Command & Control server
    - Plausible criminal workflow:
      - Compromised cards → dumps → sold → made into physical credit cards to be used in card present transactions

ARBOR NETWORKS

PoS Campaigns: Compromise Tactics

- Indicatiors suggest the following:
  - Remote Desktop with weak credentials
  - Open wireless networks including PoS machines
  - Social engineering tactics
  - Possible spear phishing attacks
  - Physical attacks (USB drives and autoruns)

ARBOR NETWORKS

Global infection – Dexter & Project Hook

24 Jan 2014

ARBOR NETWORKS

Campaign Discovery

From Bing, Matthew

Reply | Reply All | Forward | Archive | Junk | Delete

Subject **Open Directory Digest 2013-11-03** 11/2/13, 11:44 PM

To Bing, Matthew, Barr, Michael, Schwarz, Dennis, Curt Wilson Other Actions

```
Tested 272 URLs, 12 potential open directories

http://download[.]cdn[.]mozilla[.]net/pub/mozilla[.]org/firefox/releases/23[.]0/win32/en-US
http://www[.]goplayer[.]cc/original
http://www[.]soft365[.]com/hpnt/new
http://zeybor[.]biz/Crx
http://download[.]cdn[.]mozilla[.]net/pub/mozilla[.]org/firefox/releases/22[.]0/win32/en-US
http://hi[.]mybro[.]biz/fk
http://download[.]animationsoftware7[.]com/
http://get-files20[.]ru/file
http://mirror1[.]filefacts[.]com/4c341f85acff2fa726f3e79f9dfc2a21
http://www[.]doctopdfconverter[.]org/download
http://rome0[.]biz/hint
http://cdn01[.]foxitsoftware[.]com/pub/foxit/reader/desktop/win/6[.]x/6[.]0/enu
```

- ASERT Open Directory Crawler tool
  - Crawls directories seen during malware analysis
  - Discovered stolen credit card data

ARBOR NETWORKS

Campaign Discovery

- Another Dexter sample in same timeframe
  - Stored FTP credentials to upload card data

SENSITIVE: Dexter Revelation uses FTP to exfiltrate stolen data. Data files use a zip extension but are not in the clear. The Dexter binary contains credentials and the FTP site IP address in plaintext without any obfuscation. The following screenshots from IDA Pro reveal FTP credentials in the .data section of the binary and the follow-up screenshot shows the actual function using an API call to InternetConnectA.

Figure 1: *FTP Credentials obtained from MD5 18af3ebfeed704edcf35f4a56723a85d – Dexter Revelation*

```
.data:0040B174                 align 8
.data:0040B178 a80_82_78_24    db '[redacted]'          ; DATA XREF: .data:off_40B19C↓o
.data:0040B184 aAdata          db 'adata',0             ; DATA XREF: .data:off_40B1A4↓o
.data:0040B18A                 align 4
.data:0040B18C aFlinstone2004  db 'flinstone2004',0     ; DATA XREF: .data:off_40B1A8↓o
.data:0040B19A                 align 4
.data:0040B19C off_40B19C      dd offset a80_82_78_24   ; DATA XREF: sub_405AF0+5A↑r
```

ARBOR NETWORKS

ATLAS Malware Corral Tracking

Tracking several PoS+ malware families

Tag	Count	Oldest	Newest
dexter	36	2013-05-10 10:23:09	2014-01-02 09:27:20
alina	10	2013-07-19 05:27:20	2013-08-30 11:09:06
alina_v5	10	2013-06-07 03:19:37	2014-01-03 13:36:28
projecthook	6	2013-05-30 16:04:16	2013-11-02 08:36:24
vskimmer	5	2013-07-12 08:31:12	2013-08-19 17:13:37
citadel_krebs	6367	2013-04-18 11:23:19	2013-11-25 10:42:06
citadel_dplohmann	266	2013-10-02 06:53:30	2013-10-16 05:33:56
Citadel_Rain	5	2013-06-19 02:17:38	2013-10-19 05:00:30
citadel	4	2013-05-21 13:20:03	2013-05-25 05:21:45

ARBOR NETWORKS

ASERT Malware Analysis

Available Analysis Reports:

- Task-169353943 [norman.winxp.dump.inert] on 2014-08-29 @ 23:25:00
- Task-166737103 [norman.winxp.dumpless] on 2014-05-07 @ 18:46:05
- Task-166737065 [norman.winxp.dump.default] on 2014-05-07 @ 18:39:34
- Task-166736538 [norman.sandbox.default] on 2014-05-07 @ 17:13:23
- Task-164055930 [norman.sandbox.default] on 2014-03-19 @ 18:57:10
- Task-164055932 [norman.winxp.dumpless] on 2014-03-19 @ 18:02:19
- Task-164055931 [norman.winxp.dump.default] on 2014-03-19 @ 16:35:04
- Task-21773581 [norman.win7.dump.comms] on 2013-06-13 @ 08:29:10

Available Dynamic Analysis Log(s):

- Task-164055931 [dynamic.pluglog] on 2014-03-19 @ 16:35:07
- Task-166737065 [dynamic.pluglog] on 2014-05-07 @ 18:39:40
- Task-169353943 [dynamic.pluglog] on 2014-08-29 @ 23:25:19
- Task-169353943 [dynamic.tasklog] on 2014-08-29 @ 23:25:19
- Task-21773581 [dynamic.pluglog] on 2013-06-13 @ 08:29:19

Suricata Alerts:

[2807327] ETPRO TROJAN Dexter Variant (rev: 3)

Available Commentary:

- **2013-05-30 16:08:09 by dschwarz** *http://www.xylibox.com/2013/05/projecthook-ram-...* [DEL]
- **2014-03-20 08:55:05 by analyzer.strings** *String-based detection(s) Task-21773581 / Dump-...* [DEL]
- **2014-05-08 09:03:59 by analyzer.strings** *String-based detection(s) Task-166737065 / Dump...* [DEL]
- **2014-08-30 02:06:48 by analyzer.strings** *String-based detection(s) Task-169353943 / Dump...* [DEL]
- **2014-08-30 02:09:17 by analyzer.strings** *String-based detection(s) Task-169353943 / Dump...* [DEL]
- **2014-08-30 02:10:19 by analyzer.strings** *String-based*

Sample Tags:

dexter [DEL]
dloftus [DEL]
projecthook [DEL]
Add Sample Tag

Resource Package: [Download]

Sandbox Report(s): 8
Memory Dump(s): 22
Dropped File(s): 6
PCAP(s): 6
Screenshot(s): 10

3 DNS Lookup(s):

www.inf0nix.com [REP] [POL] 91.208.16.252 [REP] [POL] [PROP]
www.inf0nix.com [REP] [POL] 189.38.88.130 [REP] [POL] [PROP]
www.inf0nix.com [REP] [POL] 195.3.144.87 [REP] [POL] [PROP]

6 Connection(s):

Task-169353943:	TCP/80	www.inf0nix.com	LV	dexter_cnc [DEL]	Add Connection Tag
Task-21773581:	TCP/80	www.inf0nix.com	BR		Add Connection Tag
Task-166737103:	TCP/80	www.inf0nix.com	RU		Add Connection Tag
Task-166737065:	TCP/80	www.inf0nix.com	RU		Add Connection Tag
Task-164055931:	TCP/80	www.inf0nix.com	RU		Add Connection Tag
Task-164055932:	TCP/80	www.inf0nix.com	RU		Add Connection Tag

HTTP Request(s):

http://www.inf0nix.com/notify.php [REP] [POL]

HTTP Header Details

ARBOR NETWORKS

ASERT Response

- Notified financial sector contacts & FBI
- Conference call (financials)
- Sensitive data dumps given to financials
- TLP AMBER (need to know basis) Threat Intelligence document written and distributed to relevant parties
- Contained sensitive data and numerous indicators of Compromise (IOCs)
- IOCs useful to help compromises

ARBOR NETWORKS

Threat Intelligence Product and Blog

ASERT issued *ASERT Threat Intelligence Brief 2013-6* in a TLP AMBER and a TLP GREEN version, followed by a later blog post.

Blog post received significant attention from the press and security industry resulting in several interviews and excellent coverage.

Arbor ASERT Threat Intelligence

ASERT Threat Intelligence Brief 2013-6

Dexter Point of Sale Malware Attack Campaign Indicators

ASERT Threat Intelligence November 11, 2013

This document is TLP AMBER and is to be shared only within Arbor Networks and with others who have a need to know. This document contains very sensitive information and is not to be made public or shared further without specific permission. Please see http://www.us-cert.gov/tlp for further details on the Traffic Light Protocol regarding sensitive information sharing.

An active Point of Sale (PoS) compromise campaign designed to steal credit card data using the Dexter malware has been detected. Indicators of compromise will be provided for mitigation and detection purposes. Prior to the publication of this Threat Intelligence document, members of the FS-ISAC and major Credit Card vendors were notified. Malicious sites listed herein should not be tampered with except by authorized individuals.

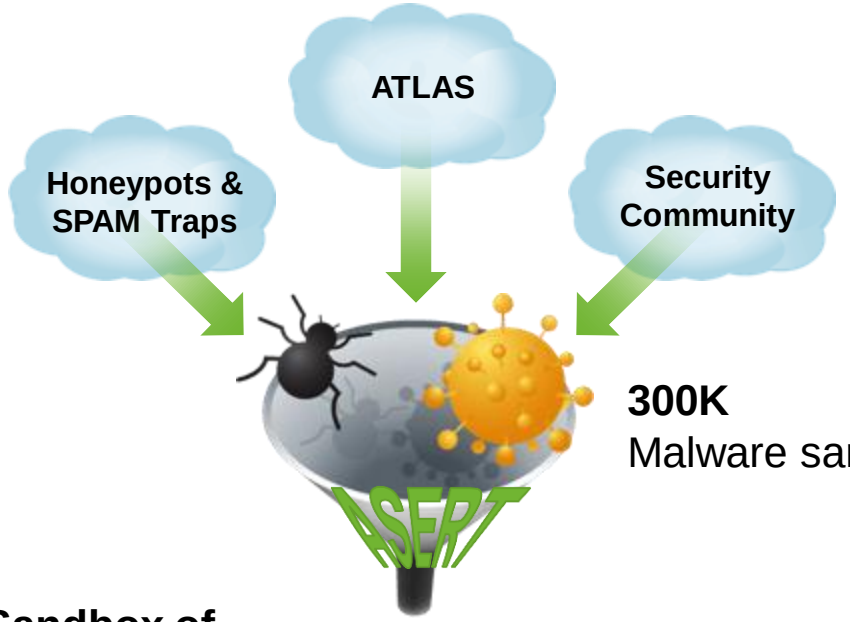
ARBOR NETWORKS

ASERT follow-up actions

- Ongoing monitoring of C&C servers to harvest data & new malware
  - ASERT & card vendors
- ASERT researchers actively tracking and reverse engineering several PoS malwares & obtaining critical insight
  - Malware classifiers for Dexter, Project Hook, Alina
  - Network indicators intended for publication for Arbor Networks products

ARBOR NETWORKS

Arbor Security Engineering Response Team



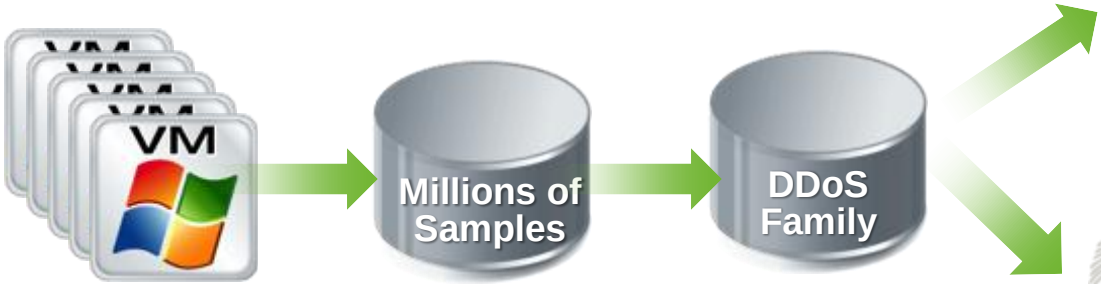
RED SKY® INSTITUTE

300K
Malware samples/day

ASERT Threat Intelligence Brief 2014-3

Dexter and Project Hook Point of Sale Malware Activity Update

Sandbox of Virtual Machines
run malware
(look for botnet C&C, files, network behavior)



Report and PCAP stored in database

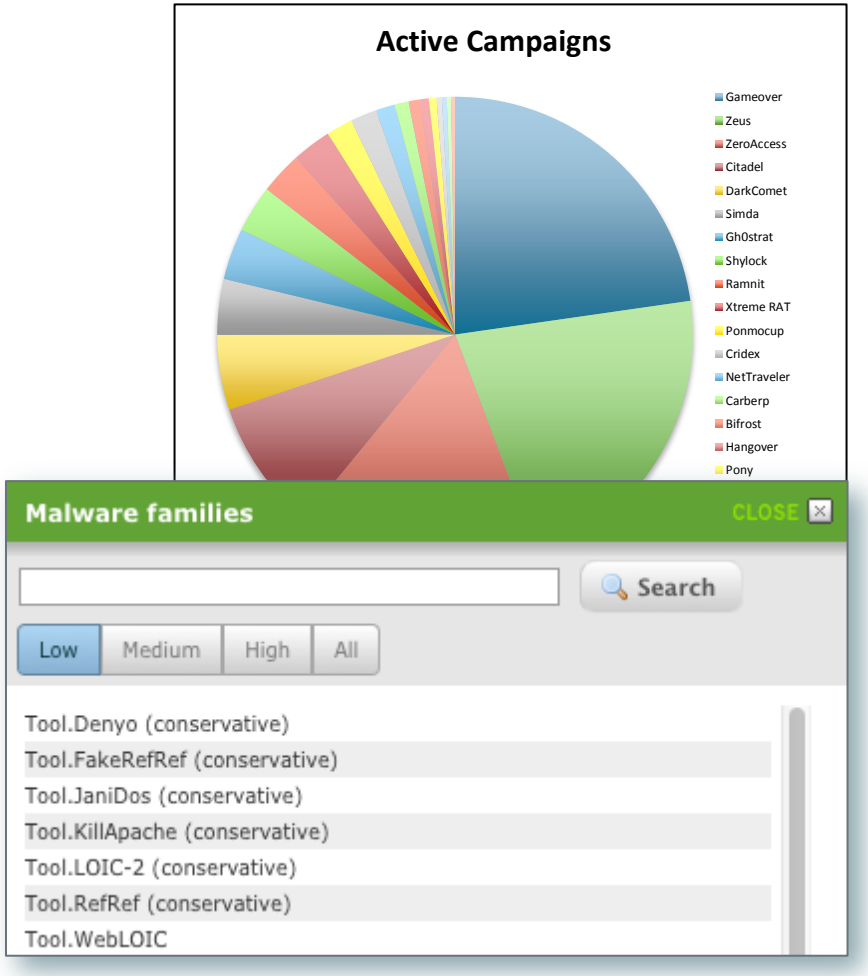
"Tracker" DDoS Attack Auto-classification and analysis every 24 hrs

AIF Policy

ARBOR® NETWORKS

How can Arbor Help? Threat Intelligence

- Utilise Arbor's visibility, expertise and experience to improve automated threat detection.
  - Threat Intelligence
    - Granular data to prevent false positives
    - Data based on in-depth research and monitoring
    - Understanding of threat 'family' + confidence = better match to risk profile



ARBOR NETWORKS

How can Arbor Help? Broad & Deep Visibility

- Leverage Flow technologies for:
  - Cost-effective, scalable visibility
  - Layer 3/4 picture of internal network
- Use packet capture for deeper visibility
  - Monitor for specific threats at network / data-centre edge.
  - Store forensic data for retrospective analysis
- Correlate
  - With actionable threat intelligence
  - Detect suspicious or malicious activities wherever they occur

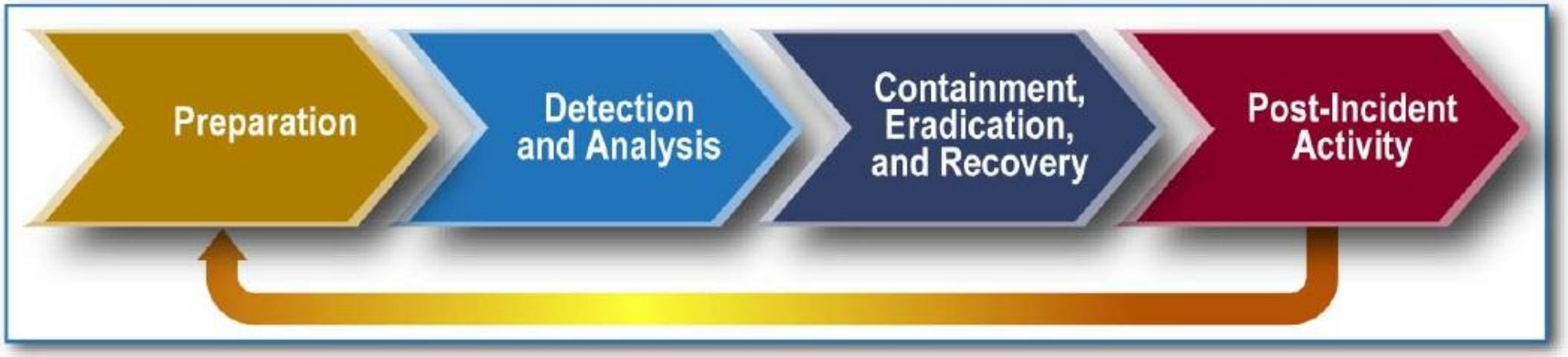
ARBOR NETWORKS

How can Arbor Help? Resource Multiplier

Comprehensive monitoring and threat detection

Situational Awareness. Augment detected events with relevant context

Provide surgical mitigation and forensic capabilities.



Source: NIST.gov

ARBOR NETWORKS

ARBOR NETWORKS

Thank You