How to detect infections in any IP asset

Mehdi Bouzoubaa
SEMEA DAMBALLA
Mehdi.bouzoubaa@damballa.com

What does Damballa FailSafe do?

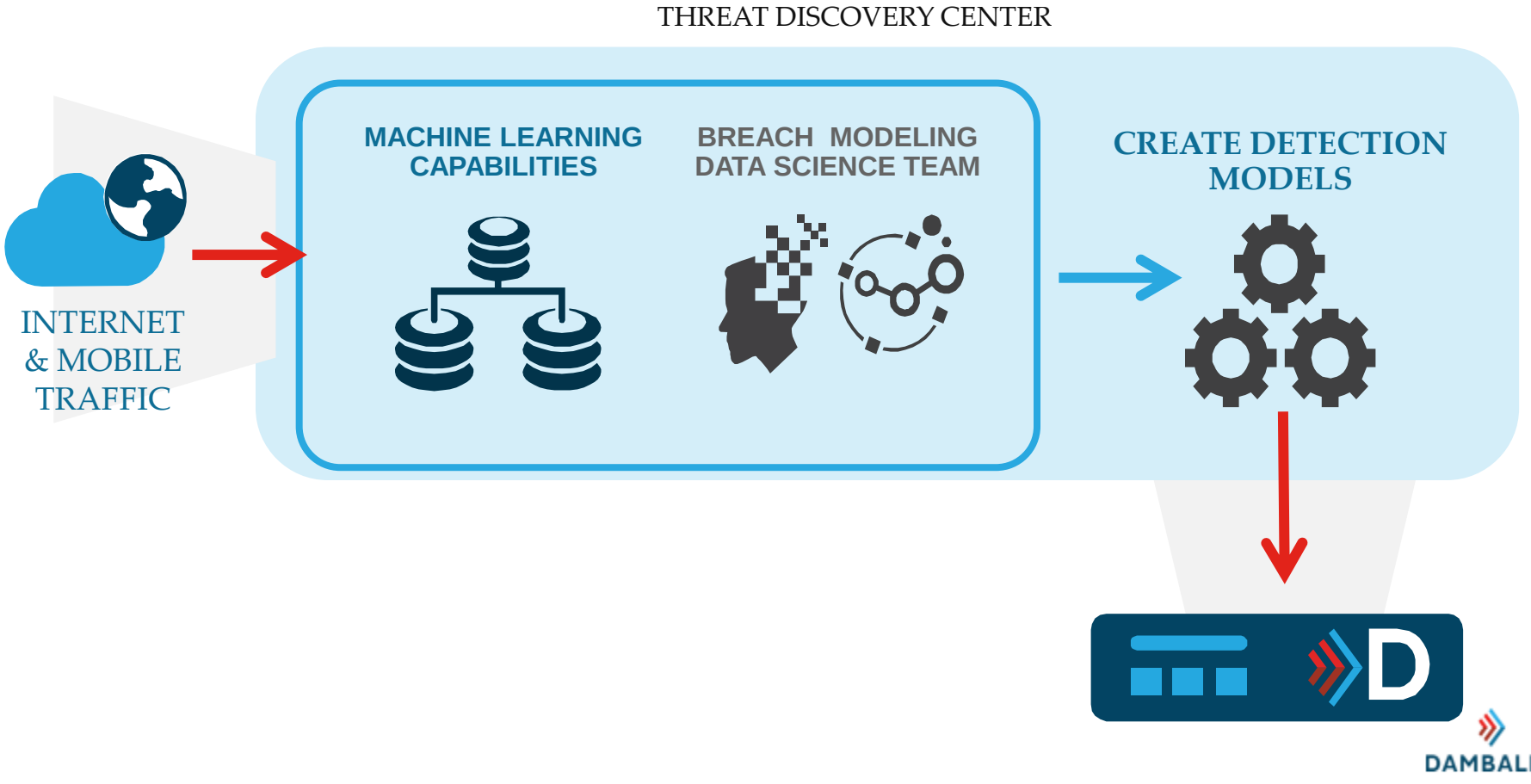
SIMPLY

Find, *Confirm*, *Prioritize*, *Evidence*

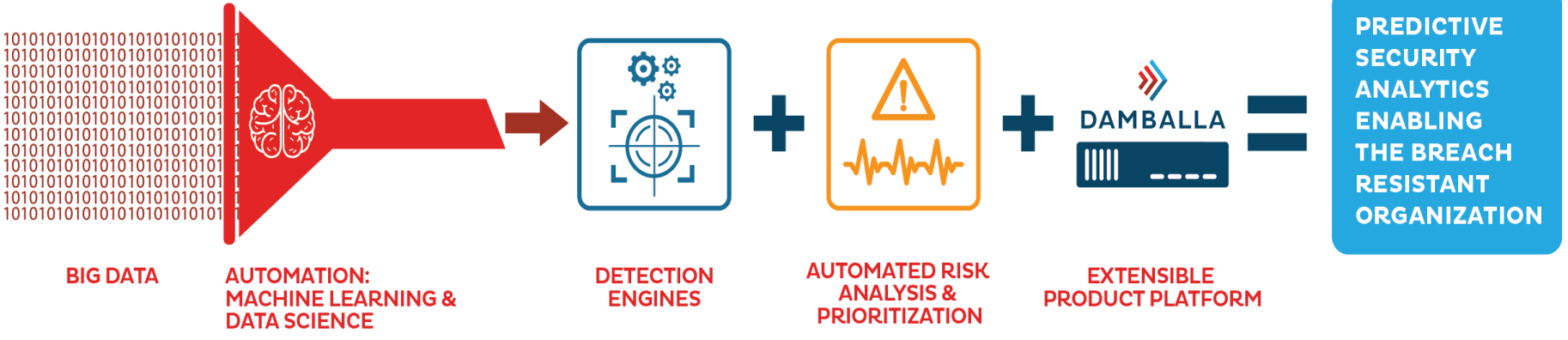
current active infections

- Find resident infections without ever seeing the malware binaries
- Confirm that malware actually infected the device (infection true positives)
- Prioritize - the same infection on two devices does not have the same priority

DAMBALLA FAILSAFE: THREAT DISCOVERY CENTER



Our Formula – Delivering Predictive Security Analytics



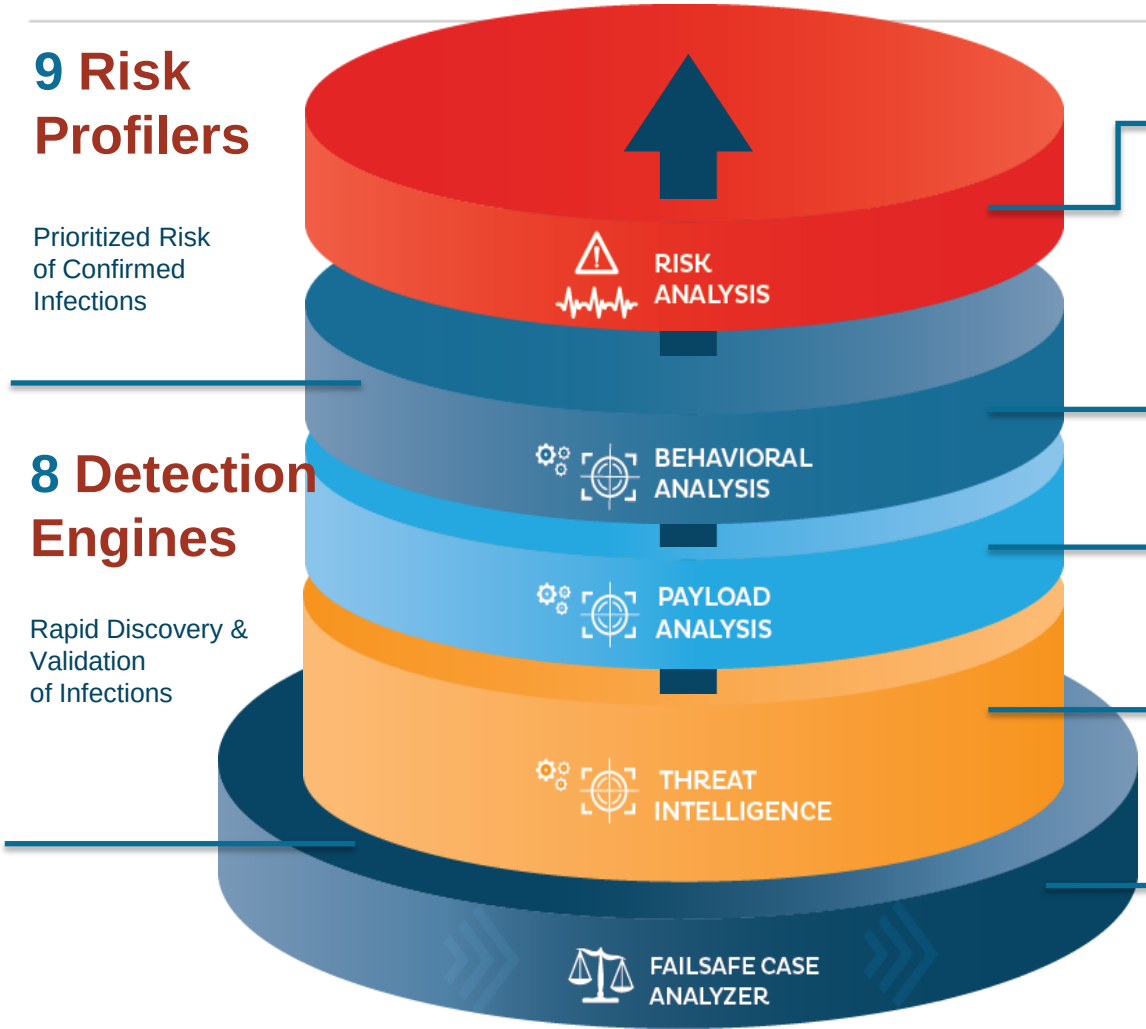
Predictive Security Analytics Platform

9 Risk Profilers

Prioritized Risk of Confirmed Infections

8 Detection Engines

Rapid Discovery & Validation of Infections



- ✓ Data Transferred
- ✓ PCAPs
- ✓ Communication Success
- ✓ Malicious File Availability
- ✓ Sequence of Events
- ✓ Importance of Endpoint
- ✓ Malware Family Intent
- ✓ Severity
- ✓ AV Coverage

Damage Potential

- Observed Activity
- Device Properties
- Threat Sophistication
- Threat Intent

- ✓ Domain Fluxing
- ✓ Automation
- ✓ Execution
- ✓ Peer-To-Peer

- Automated Malicious Activity
- Observed Evasion Tactics

- ✓ File
- ✓ Request

- Zero Day Files
- Suspicious HTTP Content

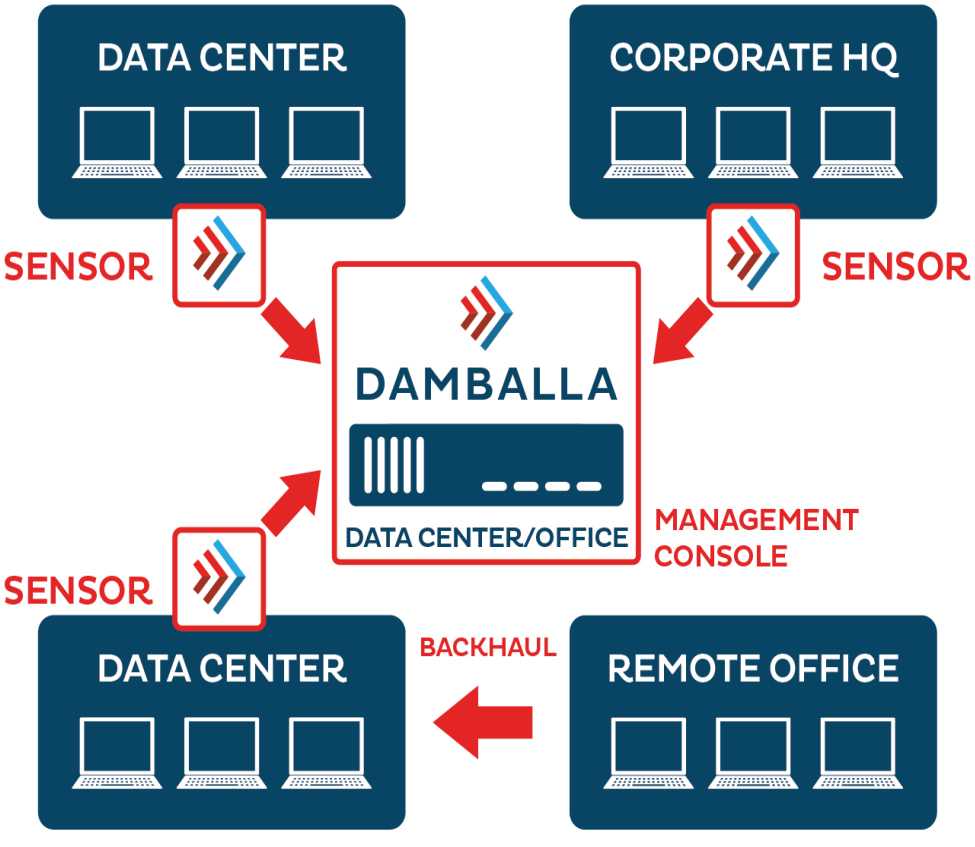
- ✓ Connection
- ✓ Query

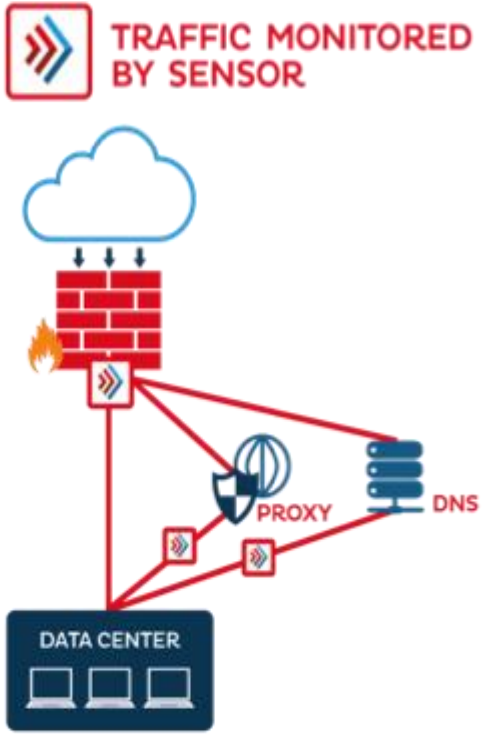
- Indicators of Compromise
- Threat Actors / Intent

Case Analyzer Platform

DAMBALLA

Damballa Failsafe Architecture

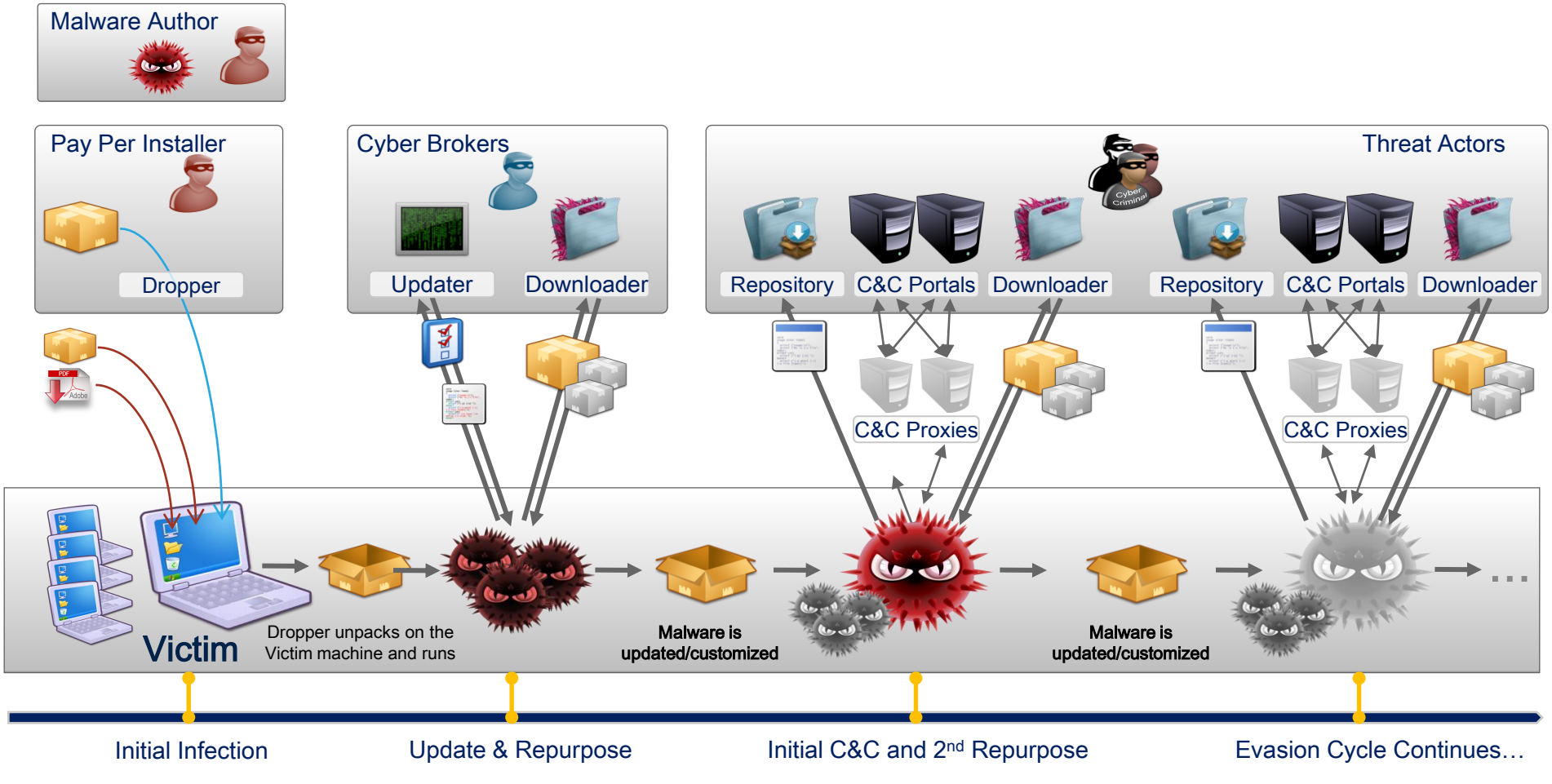




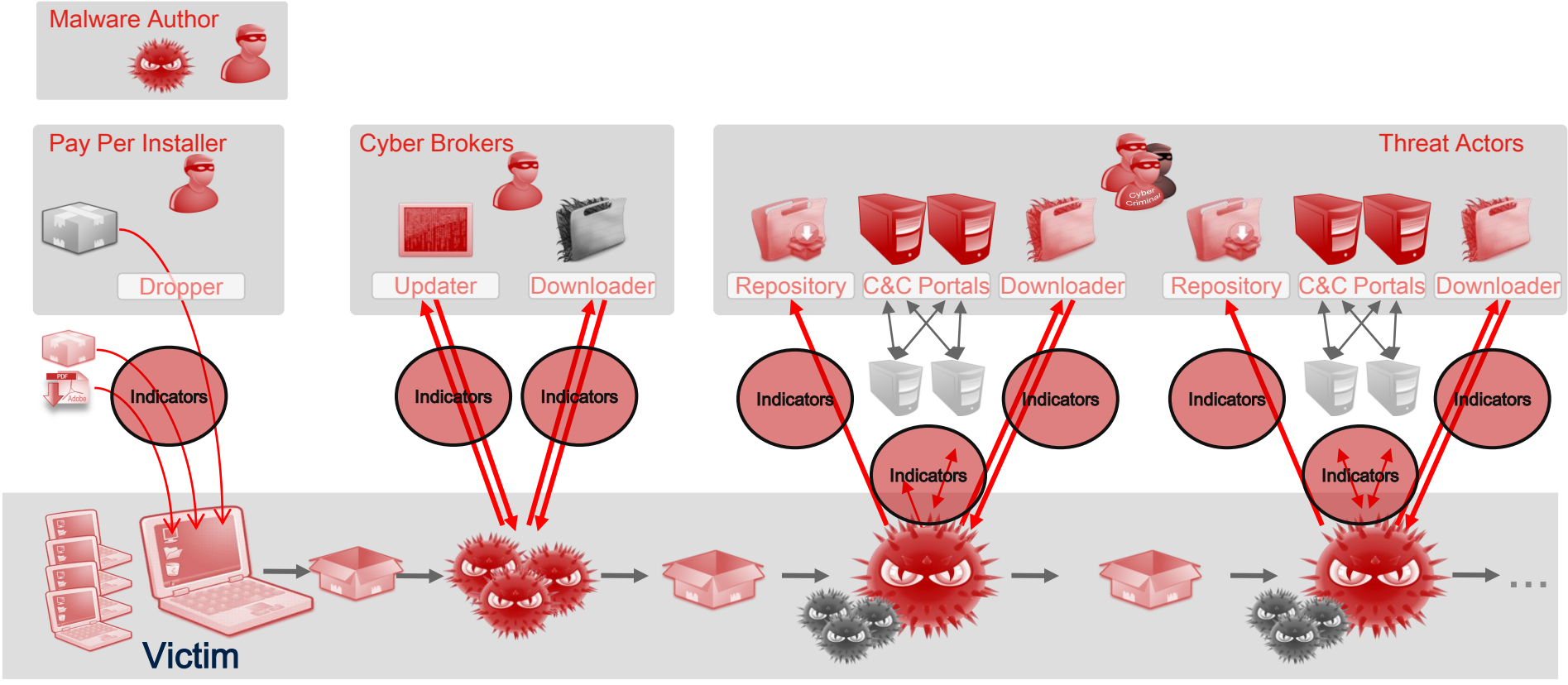
Hub & Spoke | 1 U Appliances | Out of Band

DAMBALLA

Looking at the Threat After It Bypasses Prevention



Discovering By Listening for Indicators



Who are Our Partners?
Leading Integrations & Alliances

Damballa discovers with certainty & delivers evidence so customers can pivot to…

Enrich, correlate via SIEM & Forensics

- splunk>
- IBM Q1Radar
- hp ArcSight
- NetIQ
- RSA SECURITY

Block & inform

- Bit9 + CARBON BLACK
- ForeScout
- hp TippingPoint
- IBM XGS
- BLUE COAT ProxySG Security Analytics

Accelerate & prioritize response

- EY
- pwc
- hp
- KPMG

DAMBALLA

How is Damballa Different?
Agentless Unmatched Detection & Response

Detection

- **Automate** labor-intensive task of detecting and verifying threats
- Detect **hidden threats** without prior knowledge of them
- Detect threats across **any OS**
- Detect threats regardless **of how they entered** the network
- Detect threats on **any device**

Response

- **Issue verdicts** about actual infections, not alerts
- Provide indisputable and complete **forensic evidence** about the threat(s)
- **Prioritize** devices under highest risk

DAMBALLA

DAMBALLA

Back up Slides
Anonymous
PoC Example

FINDINGS SUMMARY (February 11th - March 2nd) – Endpoint Analysis

Evidence Findings – Summary

About 60,000 End Points (Assets)

Total number of active endpoints within the environment

48 Unique Threat Actors

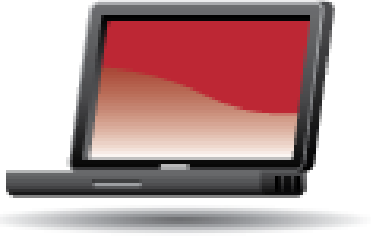
Total number of unique threats.

258 Infected Hosts

Total number of endpoints for which enough evidence of infection has been collected.

About 15 days

Amount of activity logged.



Of the approximately **60,000** endpoints seen, the detected infection represents a **0.43%** of the network (average across POCs, cross-verticals: ~1.2%).

DAMBALLA

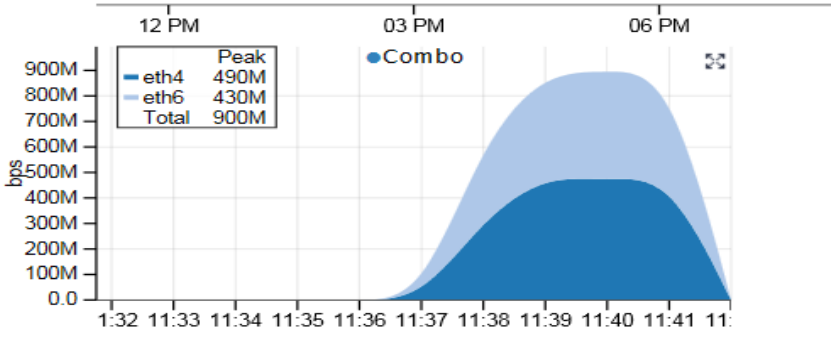
Initial discovery 11:37am after about 60 seconds...

Show 25 entries Showing 1 to 4 of 4

Download CSV | Mark as Remediated | Mark as Whitelisted | Add to Server List | Add/Change Category | Add Notes

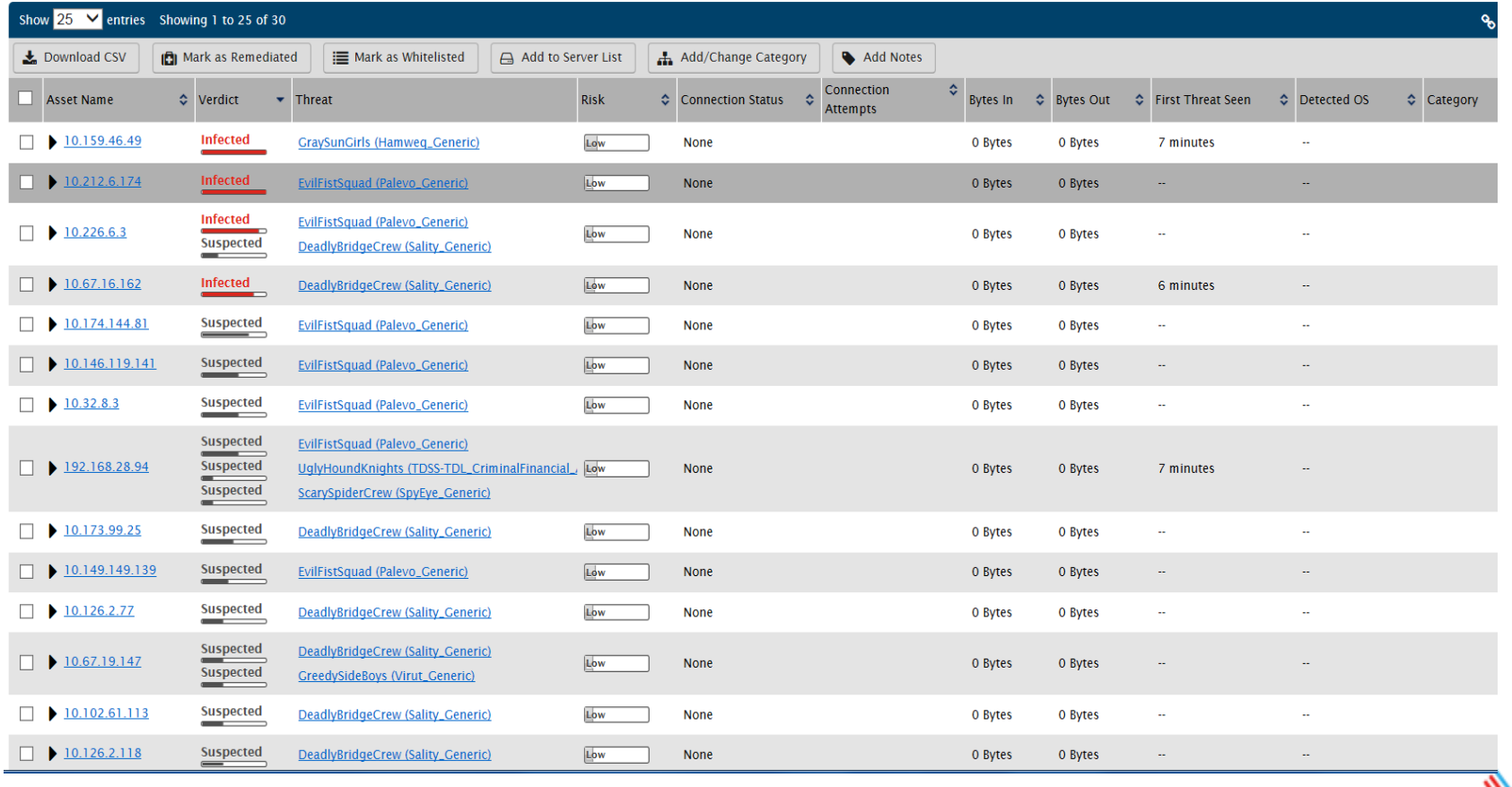
Asset Name	Verdict	Threat	Risk	Connection Status	Connection Attempts	Bytes In	Bytes O
10.4.5.7	Suspected	ThreeAlienWreckers (Citadel_Sinkhole_Microso…	Low	None		0 Bytes	0 Byte
10.159.46.49	Suspected	GraySunGirls (Hamweq_Generic)	Low	None		0 Bytes	0 Byte
192.168.28.94	Suspected	EvilFistSquad (Palevo_Generic)	Low	None		0 Bytes	0 Byte
10.67.16.162	Suspected	DeadlyBridgeCrew (Sality_Generic)	Low	None		0 Bytes	0 Byte

First Previous 1 Next Last



DAMBALLA

Initial discovery 11:44 am after about 7 minutes

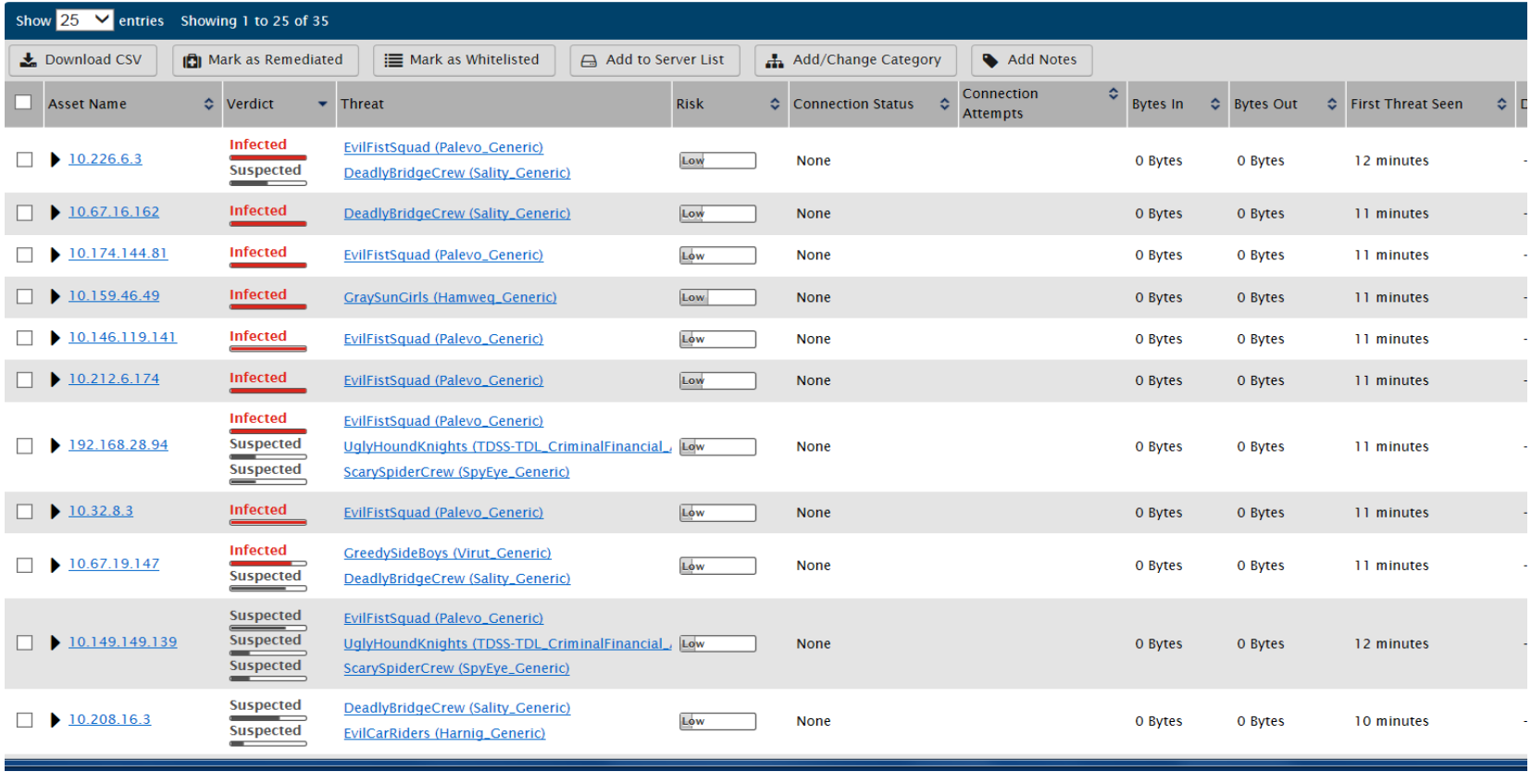


Show 25 entries Showing 1 to 25 of 30

Download CSV | Mark as Remediated | Mark as Whitelisted | Add to Server List | Add/Change Category | Add Notes

Asset Name	Verdict	Threat	Risk	Connection Status	Connection Attempts	Bytes In	Bytes Out	First Threat Seen	Detected OS	Category
10.159.46.49	Infected	GraySunGirls (Hamweq_Generic)	Low	None		0 Bytes	0 Bytes	7 minutes	--	
10.212.6.174	Infected	EvilFistSquad (Palevo_Generic)	Low	None		0 Bytes	0 Bytes	--	--	
10.226.6.3	Infected Suspected	EvilFistSquad (Palevo_Generic) DeadlyBridgeCrew (Sality_Generic)	Low	None		0 Bytes	0 Bytes	--	--	
10.67.16.162	Infected	DeadlyBridgeCrew (Sality_Generic)	Low	None		0 Bytes	0 Bytes	6 minutes	--	
10.174.144.81	Suspected	EvilFistSquad (Palevo_Generic)	Low	None		0 Bytes	0 Bytes	--	--	
10.146.119.141	Suspected	EvilFistSquad (Palevo_Generic)	Low	None		0 Bytes	0 Bytes	--	--	
10.32.8.3	Suspected	EvilFistSquad (Palevo_Generic)	Low	None		0 Bytes	0 Bytes	--	--	
192.168.28.94	Suspected Suspected Suspected	EvilFistSquad (Palevo_Generic) UglyHoundKnights (TDSS-TDL_CriminalFinancial_... ScarySpiderCrew (SpyEye_Generic)	Low	None		0 Bytes	0 Bytes	7 minutes	--	
10.173.99.25	Suspected	DeadlyBridgeCrew (Sality_Generic)	Low	None		0 Bytes	0 Bytes	--	--	
10.149.149.139	Suspected	EvilFistSquad (Palevo_Generic)	Low	None		0 Bytes	0 Bytes	--	--	
10.126.2.77	Suspected	DeadlyBridgeCrew (Sality_Generic)	Low	None		0 Bytes	0 Bytes	--	--	
10.67.19.147	Suspected Suspected	DeadlyBridgeCrew (Sality_Generic) GreedySideBoys (Virut_Generic)	Low	None		0 Bytes	0 Bytes	--	--	
10.102.61.113	Suspected	DeadlyBridgeCrew (Sality_Generic)	Low	None		0 Bytes	0 Bytes	--	--	
10.126.2.118	Suspected	DeadlyBridgeCrew (Sality_Generic)	Low	None		0 Bytes	0 Bytes	--	--	

Initial discovery 11:49 am after about 12 minutes

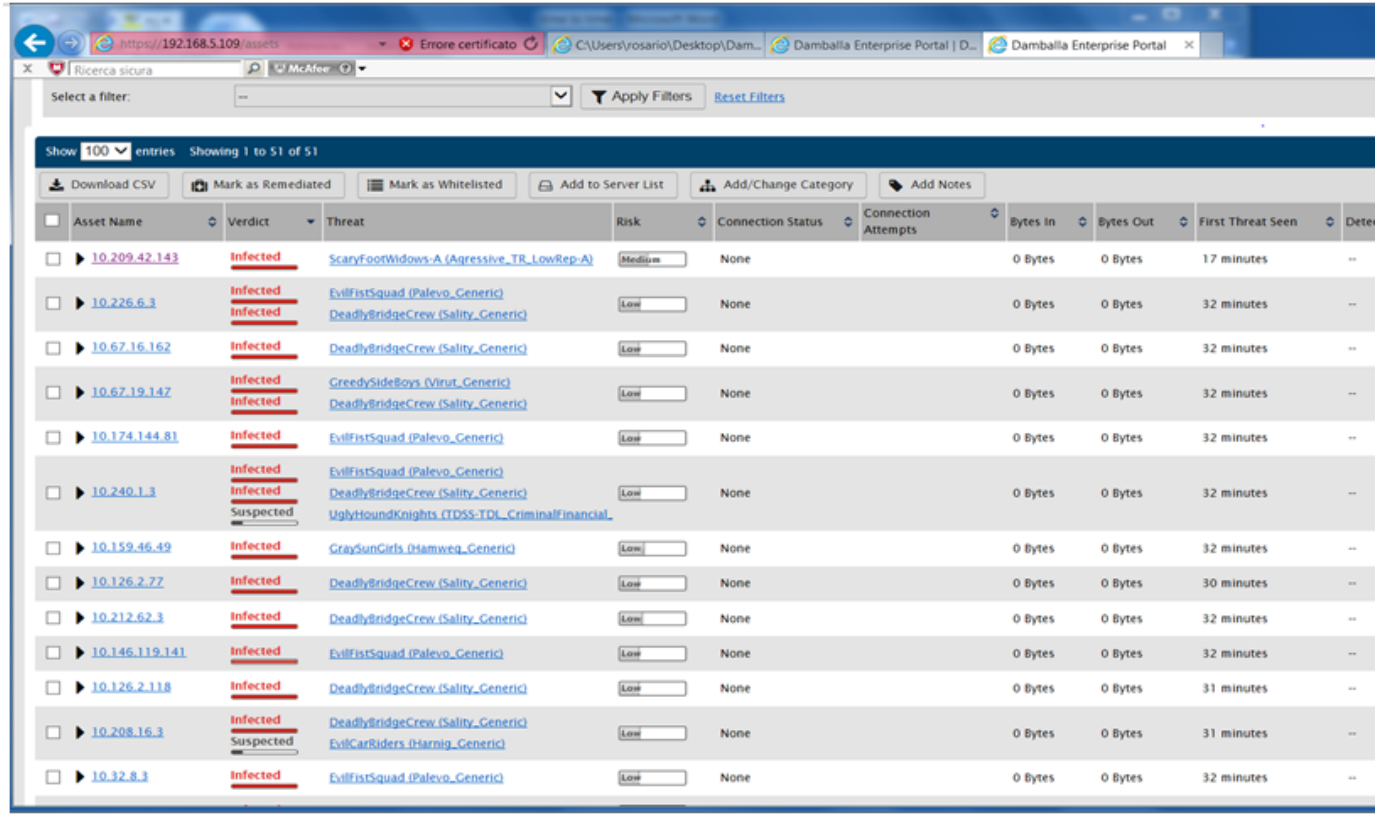


Show 25 entries Showing 1 to 25 of 35

Download CSV | Mark as Remediated | Mark as Whitelisted | Add to Server List | Add/Change Category | Add Notes

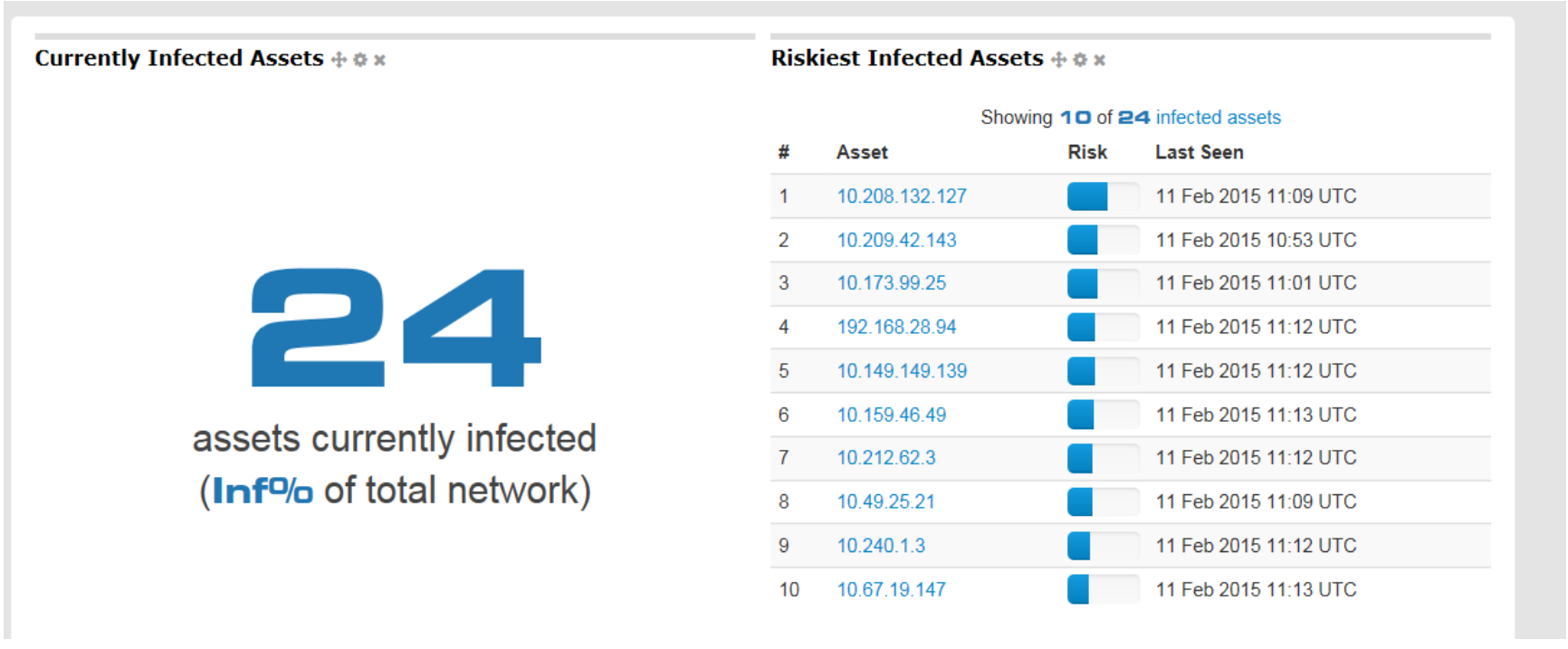
Asset Name	Verdict	Threat	Risk	Connection Status	Connection Attempts	Bytes In	Bytes Out	First Threat Seen
10.226.6.3	Infected Suspected	EvilFistSquad (Palevo_Generic) DeadlyBridgeCrew (Sality_Generic)	Low	None		0 Bytes	0 Bytes	12 minutes
10.67.16.162	Infected	DeadlyBridgeCrew (Sality_Generic)	Low	None		0 Bytes	0 Bytes	11 minutes
10.174.144.81	Infected	EvilFistSquad (Palevo_Generic)	Low	None		0 Bytes	0 Bytes	11 minutes
10.159.46.49	Infected	GraySunGirls (Hamweq_Generic)	Low	None		0 Bytes	0 Bytes	11 minutes
10.146.119.141	Infected	EvilFistSquad (Palevo_Generic)	Low	None		0 Bytes	0 Bytes	11 minutes
10.212.6.174	Infected	EvilFistSquad (Palevo_Generic)	Low	None		0 Bytes	0 Bytes	11 minutes
192.168.28.94	Infected Suspected Suspected	EvilFistSquad (Palevo_Generic) UglyHoundKnights (TDSS-TDL_CriminalFinancial_... ScarySpiderCrew (SpyEye_Generic)	Low	None		0 Bytes	0 Bytes	11 minutes
10.32.8.3	Infected	EvilFistSquad (Palevo_Generic)	Low	None		0 Bytes	0 Bytes	11 minutes
10.67.19.147	Infected Suspected	GreedySideBoys (Virut_Generic) DeadlyBridgeCrew (Sality_Generic)	Low	None		0 Bytes	0 Bytes	11 minutes
10.149.149.139	Suspected Suspected Suspected	EvilFistSquad (Palevo_Generic) UglyHoundKnights (TDSS-TDL_CriminalFinancial_... ScarySpiderCrew (SpyEye_Generic)	Low	None		0 Bytes	0 Bytes	12 minutes
10.208.16.3	Suspected Suspected	DeadlyBridgeCrew (Sality_Generic) EvilCarRiders (Harnig_Generic)	Low	None		0 Bytes	0 Bytes	10 minutes

Initial discovery 12.12 pm after about 36 minutes

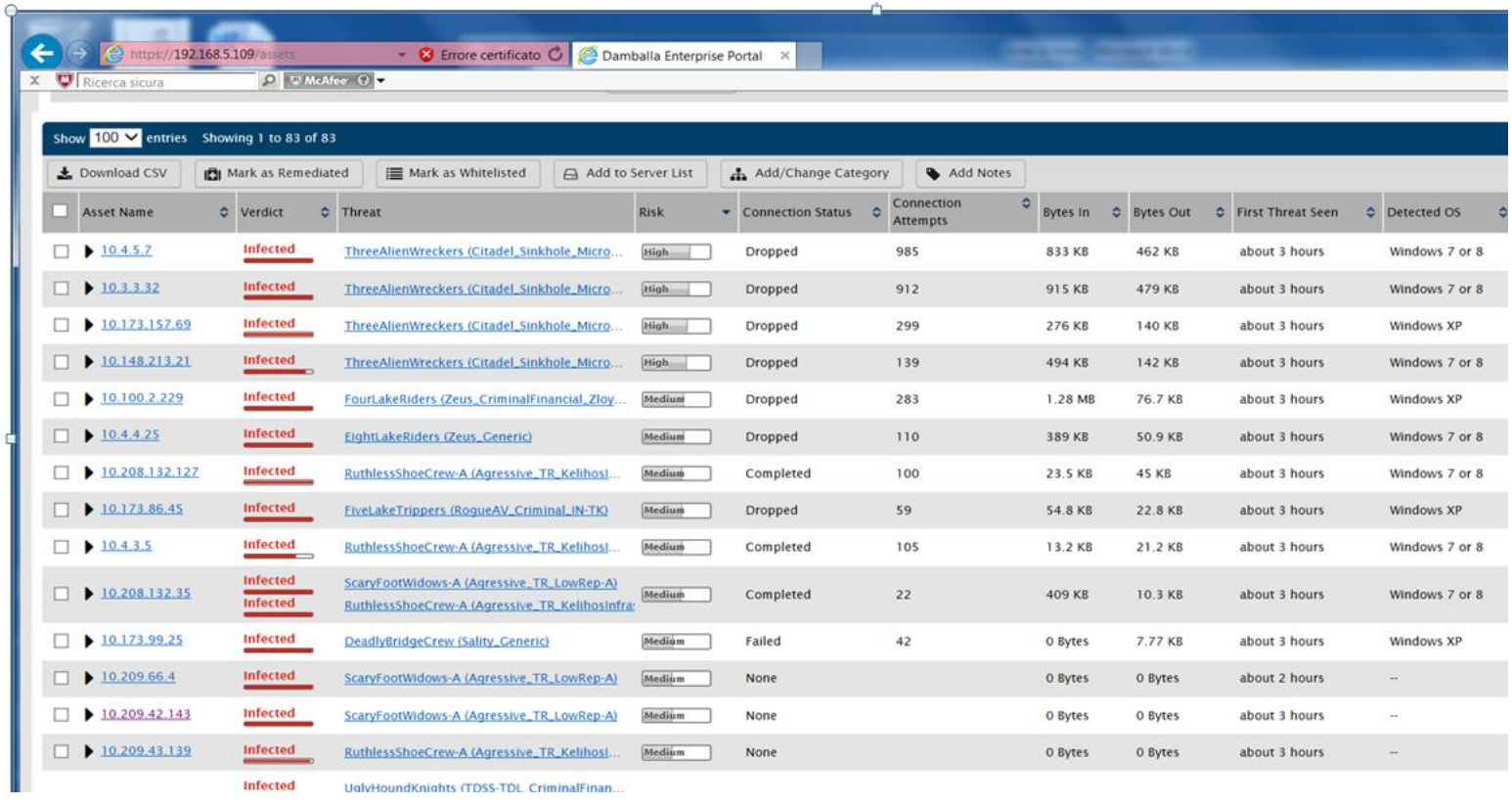


Asset Name	Verdict	Threat	Risk	Connection Status	Connection Attempts	Bytes In	Bytes Out	First Threat Seen
10.209.42.143	Infected	ScaryFootWidows-A (Agressive_TR_LowRep-A)	Medium	None		0 Bytes	0 Bytes	17 minutes
10.226.6.3	Infected Infected	EvilFistSquad (Palevo_Generic) DeadlyBridgeCrew (Sality_Generic)	Low	None		0 Bytes	0 Bytes	32 minutes
10.67.16.162	Infected	DeadlyBridgeCrew (Sality_Generic)	Low	None		0 Bytes	0 Bytes	32 minutes
10.67.19.147	Infected Infected	CreedySideBoys (Virut_Generic) DeadlyBridgeCrew (Sality_Generic)	Low	None		0 Bytes	0 Bytes	32 minutes
10.174.144.81	Infected	EvilFistSquad (Palevo_Generic)	Low	None		0 Bytes	0 Bytes	32 minutes
10.240.1.3	Infected Infected Suspected	EvilFistSquad (Palevo_Generic) DeadlyBridgeCrew (Sality_Generic) UglyHoundKnights (TDSS-TDL_CriminalFinancial_	Low	None		0 Bytes	0 Bytes	32 minutes
10.159.46.49	Infected	GraySunGirls (Hamweq_Generic)	Low	None		0 Bytes	0 Bytes	32 minutes
10.126.2.77	Infected	DeadlyBridgeCrew (Sality_Generic)	Low	None		0 Bytes	0 Bytes	30 minutes
10.212.62.3	Infected	DeadlyBridgeCrew (Sality_Generic)	Low	None		0 Bytes	0 Bytes	32 minutes
10.146.119.141	Infected	EvilFistSquad (Palevo_Generic)	Low	None		0 Bytes	0 Bytes	32 minutes
10.126.2.118	Infected	DeadlyBridgeCrew (Sality_Generic)	Low	None		0 Bytes	0 Bytes	31 minutes
10.208.16.3	Infected Suspected	DeadlyBridgeCrew (Sality_Generic) EvilCarRiders (Harnig_Generic)	Low	None		0 Bytes	0 Bytes	31 minutes
10.32.8.3	Infected	EvilFistSquad (Palevo_Generic)	Low	None		0 Bytes	0 Bytes	32 minutes

Initial discovery 12.12 pm after about 36 minutes



Initial discovery 2.36 pm after about 2 h 40



Asset Name	Verdict	Threat	Risk	Connection Status	Connection Attempts	Bytes In	Bytes Out	First Threat Seen	Detected OS
10.4.5.7	Infected	ThreeAlienWreckers (Citadel_Sinkhole_Micro...	High	Dropped	985	833 KB	462 KB	about 3 hours	Windows 7 or 8
10.3.3.32	Infected	ThreeAlienWreckers (Citadel_Sinkhole_Micro...	High	Dropped	912	915 KB	479 KB	about 3 hours	Windows 7 or 8
10.173.157.69	Infected	ThreeAlienWreckers (Citadel_Sinkhole_Micro...	High	Dropped	299	276 KB	140 KB	about 3 hours	Windows XP
10.148.213.21	Infected	ThreeAlienWreckers (Citadel_Sinkhole_Micro...	High	Dropped	139	494 KB	142 KB	about 3 hours	Windows 7 or 8
10.100.2.229	Infected	FourLakeRiders (Zeus_CriminalFinancial_Zloy...	Medium	Dropped	283	1.28 MB	76.7 KB	about 3 hours	Windows XP
10.4.4.25	Infected	EightLakeRiders (Zeus_Generic)	Medium	Dropped	110	389 KB	50.9 KB	about 3 hours	Windows 7 or 8
10.208.132.127	Infected	RuthlessShoeCrew-A (Agressive_TR_KelihosI...	Medium	Completed	100	23.5 KB	45 KB	about 3 hours	Windows 7 or 8
10.173.86.45	Infected	FiveLakeTrippers (RogueAV_Criminal_IN-TK)	Medium	Dropped	59	54.8 KB	22.8 KB	about 3 hours	Windows XP
10.4.3.5	Infected	RuthlessShoeCrew-A (Agressive_TR_KelihosI...	Medium	Completed	105	13.2 KB	21.2 KB	about 3 hours	Windows 7 or 8
10.208.132.35	Infected Infected	ScaryFootWidows-A (Agressive_TR_LowRep-A) RuthlessShoeCrew-A (Agressive_TR_KelihosInfra:	Medium	Completed	22	409 KB	10.3 KB	about 3 hours	Windows 7 or 8
10.173.99.25	Infected	DeadlyBridgeCrew (Sality_Generic)	Medium	Failed	42	0 Bytes	7.77 KB	about 3 hours	Windows XP
10.209.66.4	Infected	ScaryFootWidows-A (Agressive_TR_LowRep-A)	Medium	None		0 Bytes	0 Bytes	about 2 hours	--
10.209.42.143	Infected	ScaryFootWidows-A (Agressive_TR_LowRep-A)	Medium	None		0 Bytes	0 Bytes	about 3 hours	--
10.209.43.139	Infected	RuthlessShoeCrew-A (Agressive_TR_KelihosI...	Medium	None		0 Bytes	0 Bytes	about 3 hours	--
	Infected	UglyHoundKnights (TDSS-TDL_CriminalFinan...							

Initial discovery 2.36 pm after about 3 hours

Currently Infected Assets

55

assets currently infected

(**0.13%** of total network)

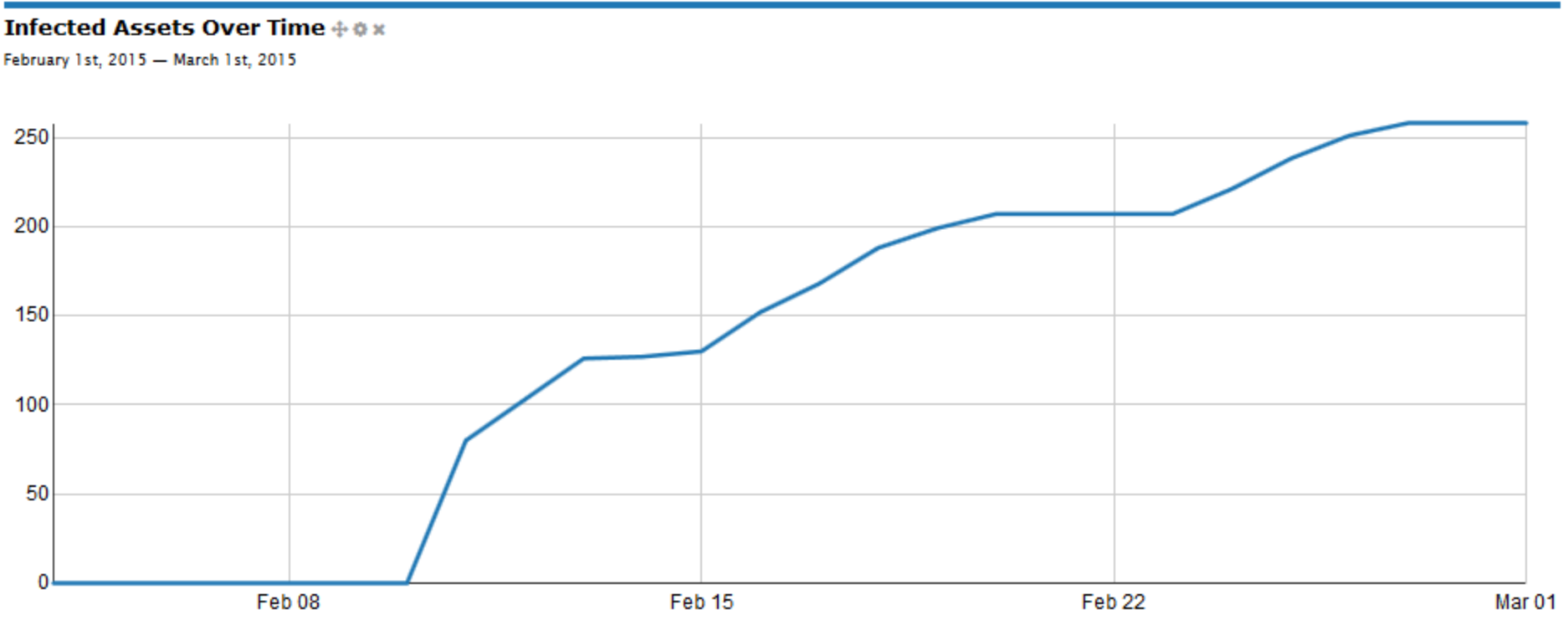
Riskiest Infected Assets

Showing **10** of **55** infected assets

#	Asset	Risk	Last Seen
1	10.4.5.7		11 Feb 2015 13:01 UTC
2	10.3.3.32		11 Feb 2015 13:34 UTC
3	10.173.157.69		11 Feb 2015 13:26 UTC
4	10.148.213.21		11 Feb 2015 11:41 UTC
5	10.100.2.229		11 Feb 2015 13:36 UTC
6	10.4.4.25		11 Feb 2015 13:30 UTC
7	10.208.132.127		11 Feb 2015 13:31 UTC
8	10.173.86.45		11 Feb 2015 13:30 UTC
9	10.4.3.5		11 Feb 2015 12:59 UTC
10	10.208.132.35		11 Feb 2015 13:26 UTC

DAMBALLA

Infected Assets Over Time (Feb 11 to March 1st)



Thank you

DAMBALLA