N1000 Network Security Appliance

For Visibility into Malware and Unknown Threats in Email, Web & File Transfers

The N1000 performs comprehensive inspection and classification of files in email, web and file transfer network traffic. It extracts and stores information on files in near real-time. The N1000 accelerates breach response with analysis of all unknown and malicious payloads as well as provides historical visibility with network context. The system enables customers to define and deploy custom detection rules to identify new threats based on new threat intelligence to counter malware attacks before damage occurs.

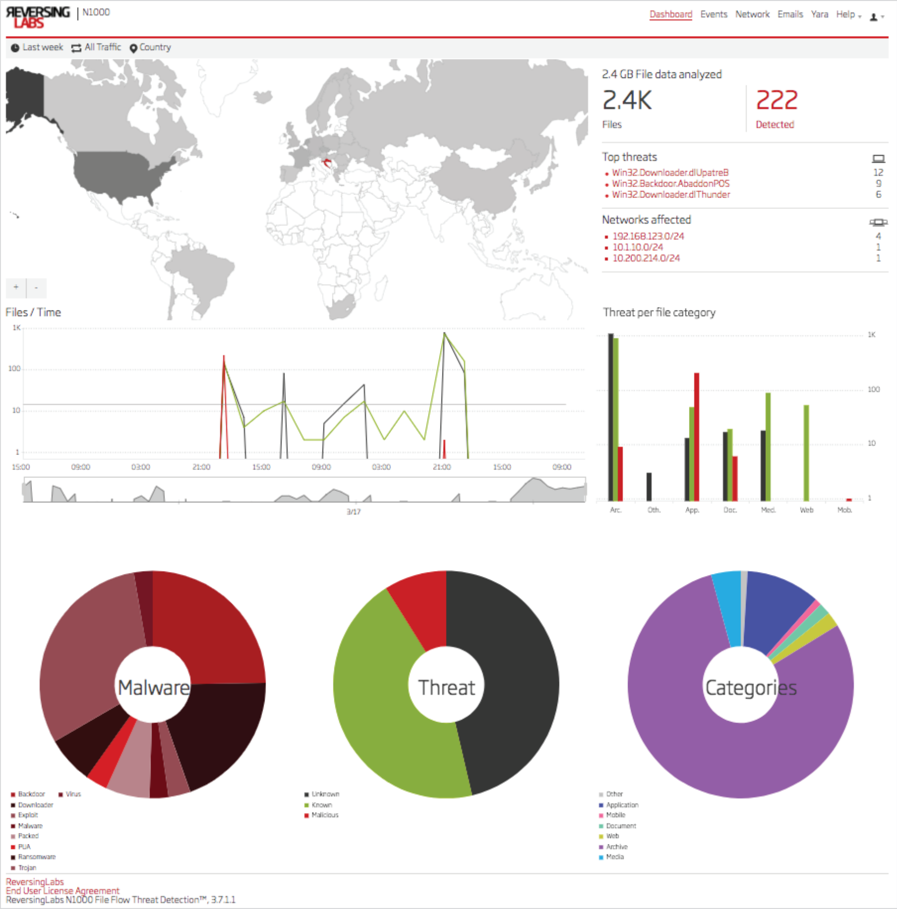
Key Benefits

- **Exceptional scale and coverage** of analyzed content at millisecond speed.
- **Provides visibility across unknown threats** in files from HTTP, SMTP and FTP traffic.
- **Identifies more than 3600 file formats** while classifying files “in flight” before they execute.
- **Performs retro-detection** by continually checking reputation on past files and alerting on status changes.
- **Enables hunting** with ReversingLabs or customer supplied YARA rules.
- **Integrates seamlessly with SIEM and analytics platforms** to supply rich file analysis data and reports.
- **Scales to high volume and deeper analysis** with TitaniumScale Enterprise Scale File Analysis for high-volume analysis, A1000 Malware Analysis Platform for deeper malware analysis & hunting, and T1000 File Reputation Appliance for on-premises privacy.

The N1000 utilizes unique ReversingLabs’ File Decomposition technology to derive detailed internal threat indicators. File Decomposition enables deep file inspection at speeds that are orders of magnitude faster than sandbox products. This allows the N1000 to extract and classify all major file formats from the network stream in near real-time. File classification utilizes up-to-date intelligence from ReversingLabs’ industry-leading File Reputation Service with a powerful rules engine to assign threat levels, names and types. The results are made available through an integrated GUI and/or customer SIEMs and analytics platforms such as Splunk and Elasticsearch for further action.

N1000 Network Threat Visualization

The N1000 enables users to view file events, access file summary and detail information, see file network context (e.g. source, destination), search by file attributes and customize threat detection with custom YARA rules.



2.4 GB File data analyzed

2.4K Files

222 Detected

Top threats

Win32.Downloader.dlUpatreB	12
Win32.Backdoor.AbaddonPOS	9
Win32.Downloader.dlThunder	6

Networks affected

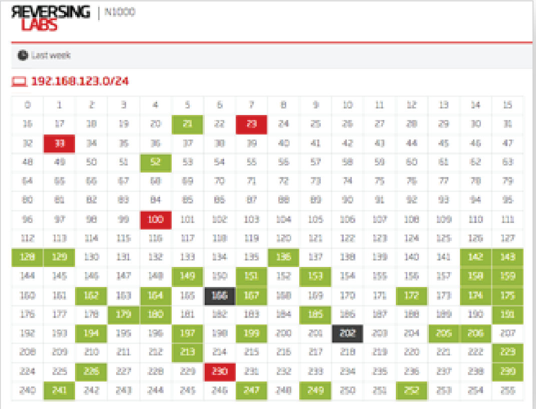
192.168.123.0/24	4
10.1.10.0/24	1
10.200.214.0/24	1

- ■ Backdoor
- ■ Virus
- ■ Downloader
- ■ Exploit
- ■ Malware
- ■ Packed
- ■ PUA
- ■ Ransomware
- ■ Trojan

- ■ Unknown
- ■ Known
- ■ Malicious

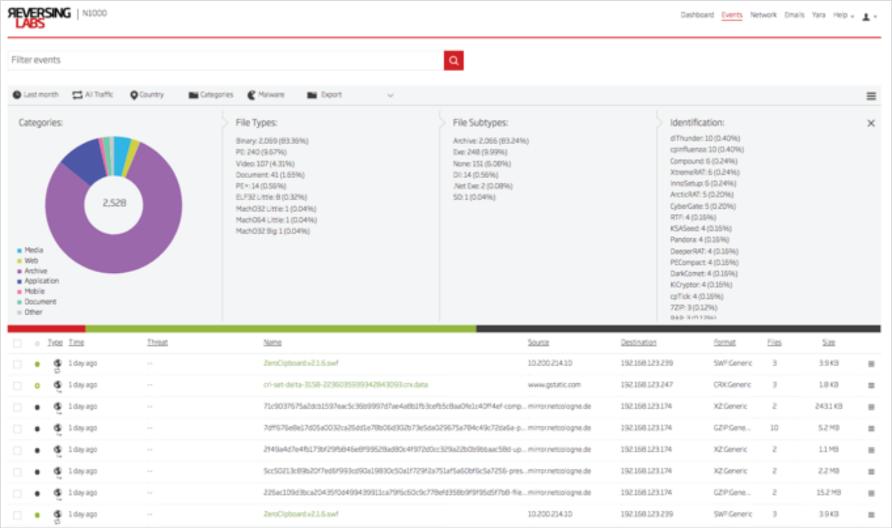
- ■ Other
- ■ Application
- ■ Mobile
- ■ Document
- ■ Web
- ■ Archive
- ■ Media

ReversingLabs
End User License Agreement
ReversingLabs N1000 File Flow Threat Detection™, 3.7.1.1



192.168.123.0/24

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111
112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143
144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159
160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175
176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191
192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207
208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223
224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239
240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255



Categories:

- ■ Media
- ■ Web
- ■ Archive
- ■ Application
- ■ Mobile
- ■ Document
- ■ Other

File Types:

Binary: 2,069 (83.35%)
PE: 240 (9.67%)
Video: 107 (4.31%)
Document: 41 (1.65%)
PE+: 14 (0.56%)
ELF32 Little: 8 (0.32%)
MachO32 Little: 1 (0.04%)
MachO64 Little: 1 (0.04%)
MachO32 Big: 1 (0.04%)

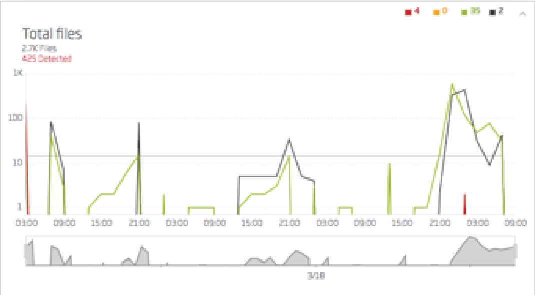
File Subtypes:

Archive: 2,066 (83.24%)
Exe: 248 (9.99%)
None: 151 (6.08%)
Dll: 14 (0.56%)
.Net Exe: 2 (0.08%)
SO: 1 (0.04%)

Identification:

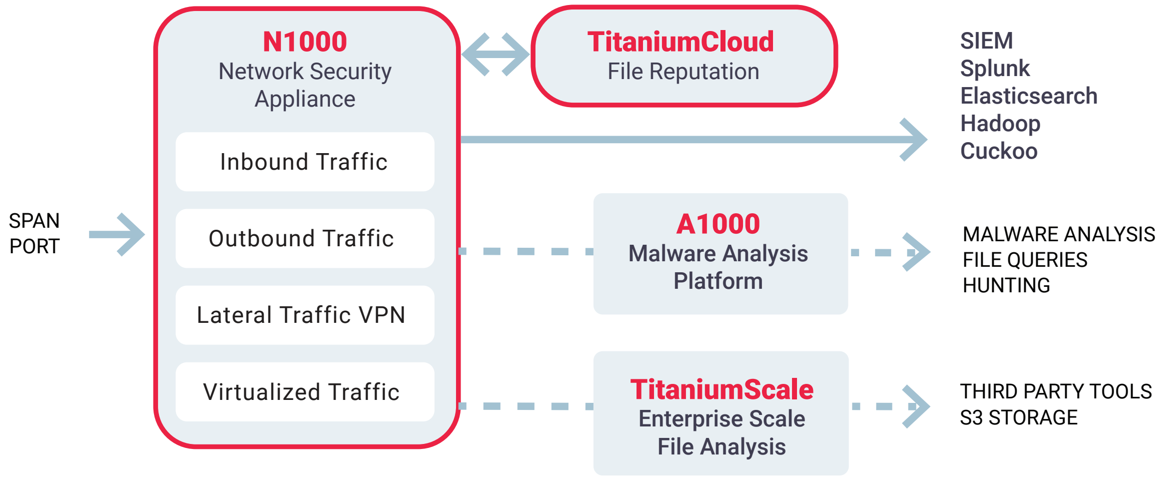
dlThunder: 10 (0.40%)
cpinfluenza: 10 (0.40%)
Compound: 6 (0.24%)
XtremeRAT: 6 (0.24%)
InnoSetup: 6 (0.24%)
ArcticRAT: 5 (0.20%)
CyberGate: 5 (0.20%)
RTF: 4 (0.16%)
KSASeed: 4 (0.16%)
Pandora: 4 (0.16%)
DeeperRAT: 4 (0.16%)
PECompact: 4 (0.16%)
DarkComet: 4 (0.16%)
KICryptor: 4 (0.16%)
cpTick: 4 (0.16%)
7ZIP: 3 (0.12%)

Type	Time	Threat	Name	Source	Destination	Format	Files	Size
	1 day ago	--	ZeroClipboard.v2.1.6.swf	10.200.214.10	192.168.123.239	SWF:Generic	3	3.9 KB
	1 day ago	--	crl-set-delta-3158-2236035939342843093.crx.data	www.gstatic.com	192.168.123.247	CRX:Generic	3	1.8 KB
	1 day ago	--	71c9037675a2dcb1597eac5c36b9997d7ae4a8b1fb3cefb5c8aa0fe1c40f4ef-comp...	mirror.netcologne.de	192.168.123.174	XZ:Generic	2	243.1 KB
	1 day ago	--	7dff676e8e17d05a0032ca26dd1e78b06d302b73e5da029675a784c49c72da6a-p...	mirror.netcologne.de	192.168.123.174	GZIP:Gene...	10	5.2 MB
	1 day ago	--	2f49a4d7e4fb173bf29fb845e8f99528ad80c4f972d0cc329a22b0b9bbaac58d-up...	mirror.netcologne.de	192.168.123.174	XZ:Generic	2	1.1 MB
	1 day ago	--	5cc50213c89b20f7ed6f993cd90a19830c50a1f729f2a751af5a60bf6c5a7256-pres...	mirror.netcologne.de	192.168.123.174	XZ:Generic	2	2.2 MB
	1 day ago	--	225ac109d3bca20435f0d4994399 11ca79f6c60c9c778efd358b9f9f95d5f7b8-file...	mirror.netcologne.de	192.168.123.174	GZIP:Gene...	2	15.2 MB
	1 day ago	--	ZeroClipboard.v2.1.6.swf	10.200.214.10	192.168.123.239	SWF:Generic	3	3.9 KB



N1000
Network Threat Detection, Classification and Hunting

The N1000 performs real-time classification and analysis of files in network traffic. With the optional TitaniumScale, the N1000 can be configured for even higher throughput applications. The information derived by the N1000 from files of interest are used to generate reports to SIEM and analytics platforms and can be automatically fed to an A1000 Malware Analysis Platform for deeper analysis.



Key N1000 Features

Network File Reputation and Analysis

- Connects to SPAN port to monitor all files traversing the network.
- Analyzes files from HTTP, FTP and SMTP traffic in near real-time.
- Processes files up to 400MB (default).
- Exceeds sandbox file processing in coverage & volume.

Threat Classification of Extracted Files

- Uses unique File Decomposition (FD) technology to assess and classify files in near real-time.
- Inspects over 360 file formats across platforms including Windows, Linux, Mac OS, Android, iOS, documents and media files.
- Reports on file activity per source, destination or file type.
- Checks TitaniumCloud file reputation service for whitelisted and blacklisted content.

Delivered as

- Hardware based or virtual machine.

Identification of Zero Day/Advanced Threats

- Recognizes polymorphic attacks by identifying functional similarity to known malware.
- Applies your custom YARA rules to all files defined for threat calculation.

Enterprise Data Integration

- Integrates file analysis logs and threat detections with SIEM or “Big Data” solutions.
- Saves files of interest via TitaniumScale or T1000 File Reputation Appliance.
- Includes Web GUI for monitoring, configuration and reporting.

ReversingLabs Integration

- Integrates with TitaniumScale for high volume applications.
- Provides input to the A1000 Malware Analysis Platform for deeper analysis and hunting.
- Connects to the T1000 File Reputation Appliance for privacy and air-gapped environments.

REVERSINGLABS

Worldwide Sales : +1.617.250.7518
sales@reversinglabs.com