

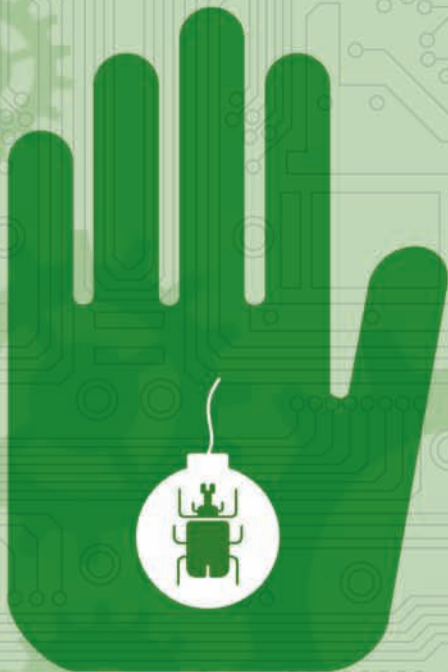


NEMESIS

NEMESIS

Advanced Compromise Protection

by **DEFENCE INTELLIGENCE**



Nemesis 2.0 – Advanced Compromise Protection

Nemesis 2.0 uses advanced network behaviour analysis in conjunction with realtime intelligence and expert threat analysis to prevent and detect compromised computers on your network. It is designed to protect computer systems against malicious software such as trojans, botnets, directed attack packages, information stealers, and other hostile code. Nemesis protects nearly all devices, regardless of operating system. Nemesis is vastly more effective than traditional security measures, and requires no additional resources.

Prevention

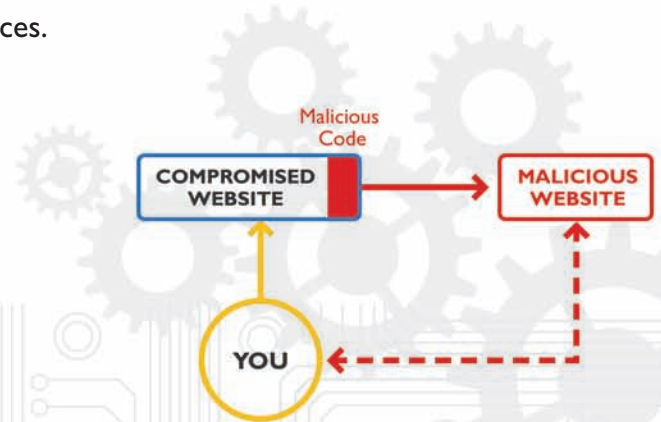
- Protects all internet devices regardless of operating system
- Prevents malware from entering your network
- Fills the vulnerability gap
- Completes your security infrastructure

Detection

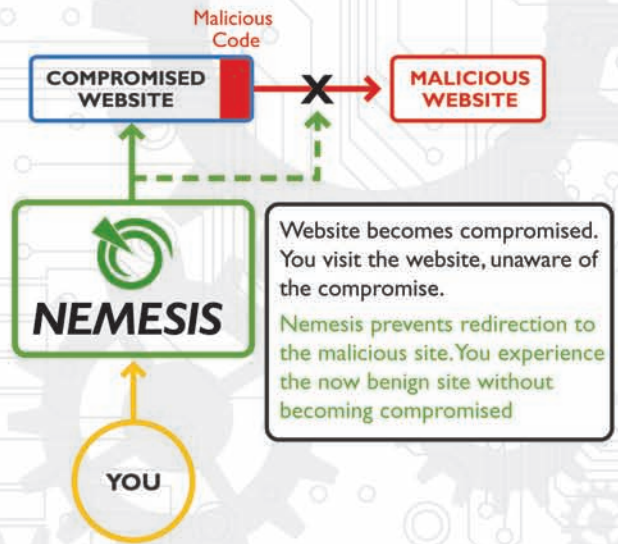
- Uses network behaviour to identify compromised systems on your network
- Alerts and reports on all malicious activity across your network

Mitigation

- Severs communication to attacker command channels rendering the malware harmless
- Prevents attackers from accessing your data or utilizing your systems for malicious purposes
- Provides your organization the time and data needed for remediation



Website becomes compromised. You visit the website, unaware of the compromise. You are redirected to a malicious site and now you are also compromised.



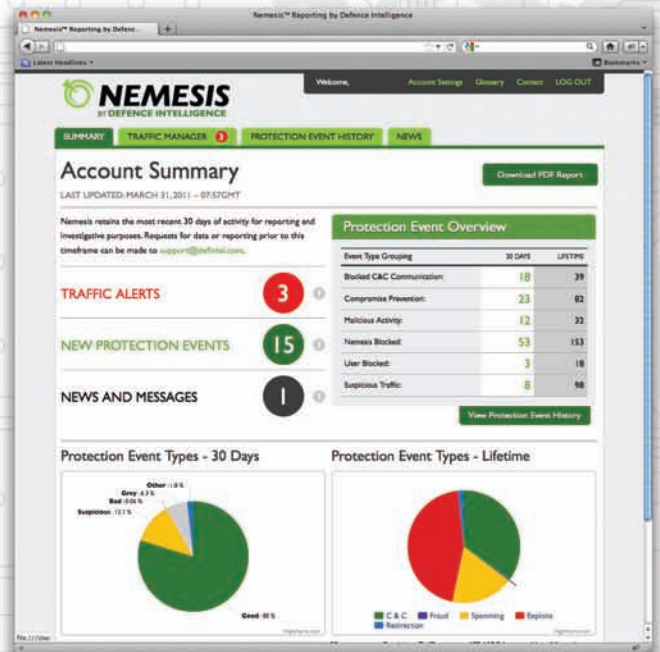
Website becomes compromised. You visit the website, unaware of the compromise. Nemesis prevents redirection to the malicious site. You experience the now benign site without becoming compromised.

Nemesis 2.0 – Advanced Compromise Protection

Nemesis 2.0 has improved compromise detection and protection capabilities, with a powerful web based management console. Create user defined blocking rules, search and filter through all the Nemesis protection event details, and generate network summary reports with ease.

Nemesis 2.0 Features

- Improved compromise detection and protection capabilities
- A web based management console that provides real time awareness of malicious activity on your network
- User defined rule creation to immediately block suspicious network communication
- Event history search and custom filtering options to find details behind every Nemesis protection event
- Easy summary and situational reporting generation and download



The screenshot shows the 'Protection Event History' page. It includes a 'FILTERS' sidebar on the left with options for 'DOMAIN', 'DATE RANGE', 'TIME OF DAY', 'PRESET FILTERS', 'EVENT TYPE', and 'STATUS'. The main area displays a table of events with columns for 'Domain', 'Query Time', 'Event Type', 'IP', and 'Status'. The table shows a list of events for various domains like 'domana.com' and 'domamb.com' with event types such as 'Phishing', 'Malware', 'C&C', 'Fraud', 'Suspicious Traffic', and 'User Blocked'.

Domain	Query Time	Event Type	IP	Status
domana.com	Feb 4, 2011 - 12:00pm	Malware	192.168.0.1	Blocked
domamb.com	Feb 4, 2011 - 12:00pm	Phishing	192.168.0.1	Blocked
domanc.com	Feb 4, 2011 - 12:00pm	Redirection	192.168.0.1	Blocked
domand.com	Feb 4, 2011 - 12:00pm	C&C	192.168.0.1	Blocked
domane.com	Feb 4, 2011 - 12:00pm	Fraud	192.168.0.1	Blocked
domanf.com	Feb 4, 2011 - 12:00pm	Suspicious Traffic	192.168.0.1	Allowed
domanl.com	Feb 4, 2011 - 12:00pm	Phishing	192.168.0.1	Blocked
domanm.com	Feb 4, 2011 - 12:00pm	Malware	192.168.0.1	Blocked
domann.com	Feb 4, 2011 - 12:00pm	Phishing	192.168.0.1	Blocked
domano.com	Feb 4, 2011 - 12:00pm	Redirection	192.168.0.1	Blocked
domanp.com	Feb 4, 2011 - 12:00pm	C&C	192.168.0.1	Blocked
domanq.com	Feb 4, 2011 - 12:00pm	Fraud	192.168.0.1	Blocked

The screenshot shows the 'Traffic Manager' page. It features a 'Traffic Alerts' section with a table of alerts for domains like 'domana.com' and 'domamb.com'. Below this is a 'User Defined Rules (179)' section with a table of rules for the same domains. The tables include columns for 'Domain', 'Query Count', 'Last Seen', 'Event Type', 'Status', and 'Rule Options'.

Domain	Query Count	Last Seen	Event Type	Status	Rule Options
domana.com	14	Feb 4, 2011 - 12:00pm	Suspicious Traffic	Allowed	Block Allow Delete
domamb.com	14	Feb 4, 2011 - 12:00pm	Suspicious Traffic	Allowed	Block Allow Delete
domana.com	14	Feb 4, 2011 - 12:00pm	Suspicious Traffic	Allowed	Block Allow Delete

Maelstrom – Analysis Engine

At the heart of the Nemesis system, is our revolutionary analysis engine, Maelstrom. This engine utilizes groundbreaking network behaviour analysis and anomaly technology to identify malicious software of all types. Maelstrom can analyze 40,000 unique binaries per day and is infinitely scaleable.

- Strategically placed sensors on the internet provide global visibility into malicious online activity
- Maelstrom identifies over 15 million malicious domains per year
- Maelstrom can analyze binaries in far less time than signature based tools
- Near zero false positives
- Up to the minute data feeds of malicious domains

From the first international, interagency prosecution of a cyber crime – to the discovery of one of the world’s largest botnets, *Defence Intelligence* is always at the forefront of the battle against online crime.

Founded in 2008, Defence Intelligence is an Ottawa based information security firm specializing in advanced compromise protection. Perhaps best known for discovering and dismantling the Mariposa botnet, Defence Intelligence has received international acclaim and been awarded the Global Hero Award by the Digital Crimes Consortium.

A passionate group of security experts, Defence Intelligence combines global threat data, research partnerships, analysis and proprietary tools and techniques to provide the most effective compromise protection solutions available.

Our team members are regularly featured as experts on CNN, ABC, BBC, NBC, CBS, CBC, Fox, and for publications such as The Wall Street Journal, USA Today, The Washington Post, The Globe and Mail, and The National Post.

For more information about our Nemesis Service or any of our other advanced compromise prevention/detection offers please contact us at :

**613.591.8985 or
info@defintel.com**



180 Preston Street – Third Floor
Ottawa, Ontario, Canada
K1R 7P9

1.877.331.6835

www.defintel.com