



HEIMDAL
SECURITY

Protects what others can't

About Heimdal Security



Leading product and intelligence

Appraised by the FBI, working with EUROPOL and endorsed by NC3

Defcon CTF World champions

Developed and evolved by the best of the industry

Superb service and support

Recommended by our customers for our great service and support

Our ground-breaking intelligence alerts have been featured in media such as:



Europe's most educational cyber security blog

Endorsed by Law enforcement



→ <https://www.theguardian.com/technology/2014/jun/04/cryptolocker-ransomw>

Danish security firm Heimdal Security says that the operation against Cryptolocker has been a success based on early data. The company has been praised by the FBI for its technical assistance in tracking the malware.

The company says that in early May, it was seeing as many as 8,000 new Cryptolocker infections every day, but that this had now dropped to almost zero following the global police operation.

The Cryptolocker operation has been a success looking at early data, said Danish security firm Heimdal Security, which was commended by the FBI for its technical assistance in tracking the malware. Heimdal warned that it does not have access to data on all networks related to Cryptolocker, however.

Despite these positive signs, it's quite possible that Cryptolocker will make a comeback as soon as its creators rebuild their operation. This is why the UK's National Crime Agency has given a two-week deadline for people to update their

→ www.tripwire.com/state-of-security/security-data-protection/cyber-security/stampado

Innovation never ceases in the RaaS world. Case in point, internet security firm Heimdal Security recently **detected** a new ransomware-as-a-service being advertised on the digital underground.

Those who created the RaaS, which goes by the name "Stampado," are marketing it to customers who can't afford a license for other, better-known ransomware families. As they explain in a slightly awkward, grammatically incorrect sales pitch:

"You always wanted a Ransomware but never wanted to pay Hundreds of dollars for it? This list is for you! Stampado is a cheap and easy-to-manage ransomware, developed by me and my team. It's meant to be really easy-to-use. You'll not need a host. All you will need is an email account."

For 39 USD, Stampado's authors give customers a lifetime license to the ransomware.

Andra Zaharia, a security specialist at Heimdal, explains this low price is strategic.

As **quoted** by *International Business Times*:

The power of Heimdal is the intelligence

At Heimdal, we gather our leading intelligence from a variety of sources in order to combat cyber threats:

- Penetrating and infiltrating malware infrastructure
- Tracking cybercriminal infrastructure
- Sinkholing
- Domain monitoring
- Zero hour monitoring
- Attack analysis
- Cracking Domain generation algorithms (DGA's)
- Reversing Malware samples

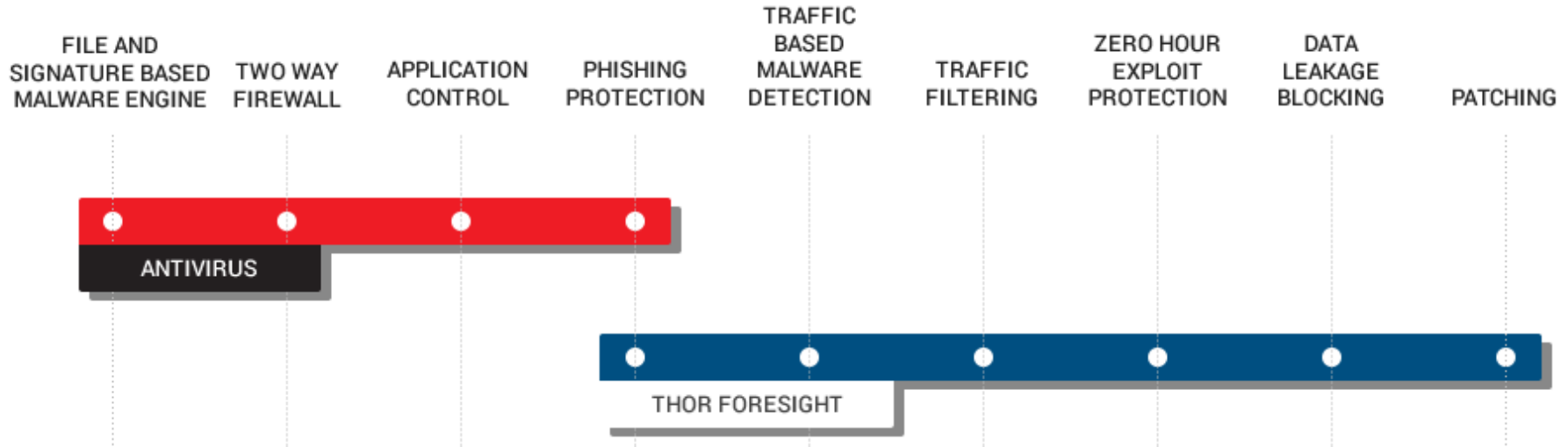


**Close vulnerabilities, be
compliant and add unique
threat prevention to stop**

Ransomware
APTs
Financial Fraud
Data leaks
Exploits

Before they do damage!

Thor Foresight as an Antivirus Complement



Mitigation and Prevention

Antivirus products and Thor Foresight **complement** each other. Leading antivirus products offer code threat detection and mitigation, and the core focus is after the system is compromised. Thor Foresight is the opposite, offering unique **attack or leakage prevention** capabilities and traffic layer and vulnerability prevention layers.

What is the difference ?

Thor Foresight focuses on network layer communication and uses vulnerability management **stop attacks before they penetrate**. Antivirus products focus on scanning file and memory for resident threats and code injection after it has penetrated. Thor Foresight is proactive, where antivirus is reactive.

Works with any Antivirus ?

Yes, Thor Foresight works with any antivirus engine on the market. Our unique threat prevention engines, will stop new 2nd generation attacks that no antivirus is able to block. Thor Foresight is the unique **next generation prevention** that will add to any existing endpoint security you have.

Virustotal.com (Google)



Search or scan a URL, IP address, domain, or file hash



Sign in



3 / 59

3 engines detected this file

SHA-256 d9679b0846140863a0338b05c1442f5a87e01a1251f4081e4a01ac5aa7872553
File name f03bea1ab5ce09c23c147f838b4e8b8d.zip
File size 9 KB
Last analysis 2018-02-01 20:15:04 UTC

Detection

Details

Relations

Community

Arcabit



Exploit.CVE-2017-11882.Gen

Qihoo-360



virus.exp.21711882.gen

TrendMicro-HouseCall



Suspicious_GEN.F47V0125

Ad-Aware



Clean

AegisLab



Clean

AhnLab-V3



Clean

Alibaba



Clean

ALYac



Clean

Antiy-AVL



Clean

Avast



Clean

Avast Mobile Security



Clean

AVG



Clean

Avira



Clean

AVware



Clean

Baidu



Clean

BitDefender



Clean

Bkav



Clean

CAT-QuickHeal



Clean

ClamAV



Clean

CMC



Clean

Comodo




Clean

Cyren



Clean

How Hackers Broke Equifax: Exploiting A Patchable Vulnerability



Thomas Fox-Brewster Forbes Staff
Sep 14, 2017, 03:22am • 10,354 views • #CyberSecurity






Unique 2-Way Traffic Filtering Engine

Blocks network communication to mitigate Zero Hour exploits, **Ransomware C&C's**, next-gen attacks and **data leakages**. Using our ground-breaking **Threat To Process Correlation** technology, we can identify attacking processes and provide **HIPS** capabilities for endpoints.

The  DarkLayer GUARD™ engine supports fully customizable white/black listing.

Detect threats that Antivirus and Code scanners can't

By tracking device-to-infrastructure communication **VECTOR**  DETECTION™ will detect 2nd generation malware strains that no other product can, effectively providing **HIDS**. Using Machine Learning (MLD) and Indicators of compromise/attack (IOA/IOC) this is a unique add-on to any other form of endpoint security. Accredited by **FBI, Europol** and **USDOJ**

Preemptive Vulnerability Management

Achieve Compliance, Mitigate exploits, - Close vulnerabilities and Install software anywhere in the world. **Zero setup, automatic, silent** and **on-the-fly** updates of your software from secure servers anywhere on the globe. X-ploit Resilience is a key security measure as exploits are used in **85% of all attacks***.

Works in any Windows environment

The Thor Product is compatible with any Windows client environment from Windows 7 to 10, VM Ware and Hyper V hosted environments.

Why Thor Foresight ?

Fits into any environment

Works with any security product, because it is different and has no hardware conflict

Adds to any Antivirus

Antivirus product is code focused, whether it is signature, behavior, kernel or exploits. Thor Foresight has no code focus, but utilizes traffic to block attacks and enables you to see software used to attack the device at **process level**.

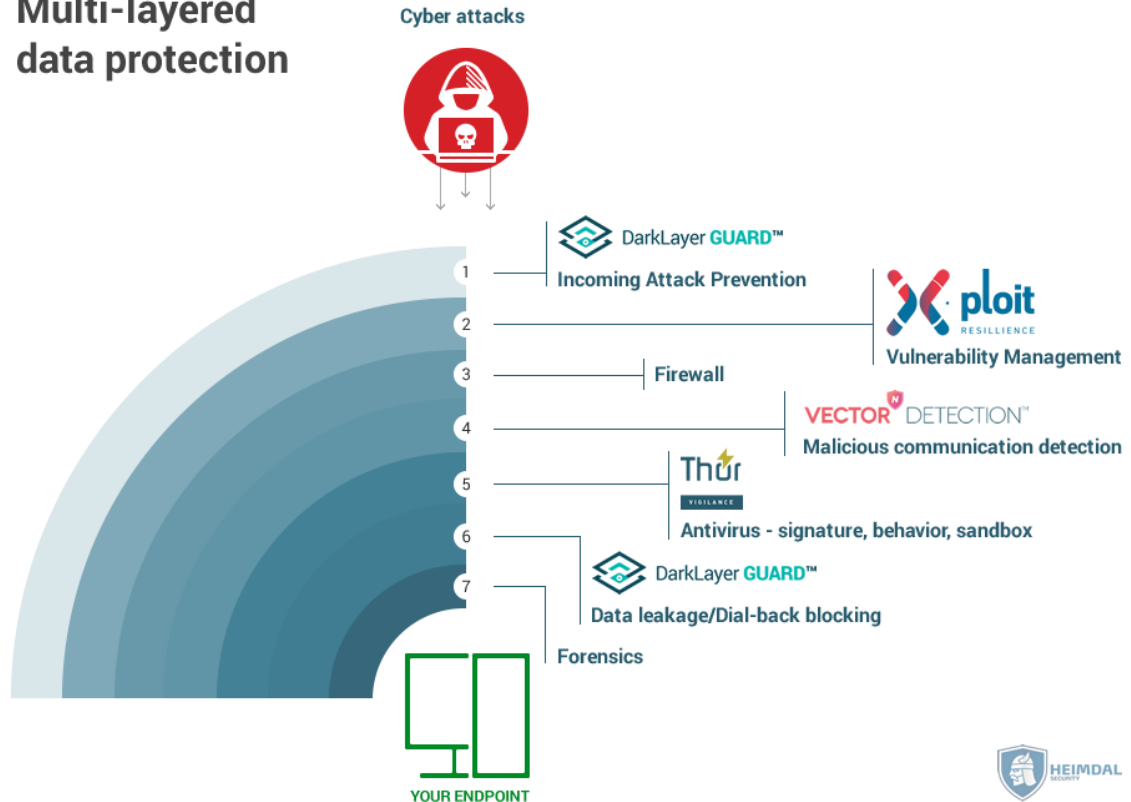
Enriches Perimeter Security

Firewalls work at port and packet inspection level to stop threats coming in. Thor Foresight works at device-to-infrastructure level to block threats coming in or data going out. Thor Foresight can also **enrich any firewall** with process and user data for easy forensic.

Adds to any Security software

Regardless of your current security offering, you will find that the core focus is reactively centered, Thor Foresight is, however, **proactively focused**.

Multi-layered data protection





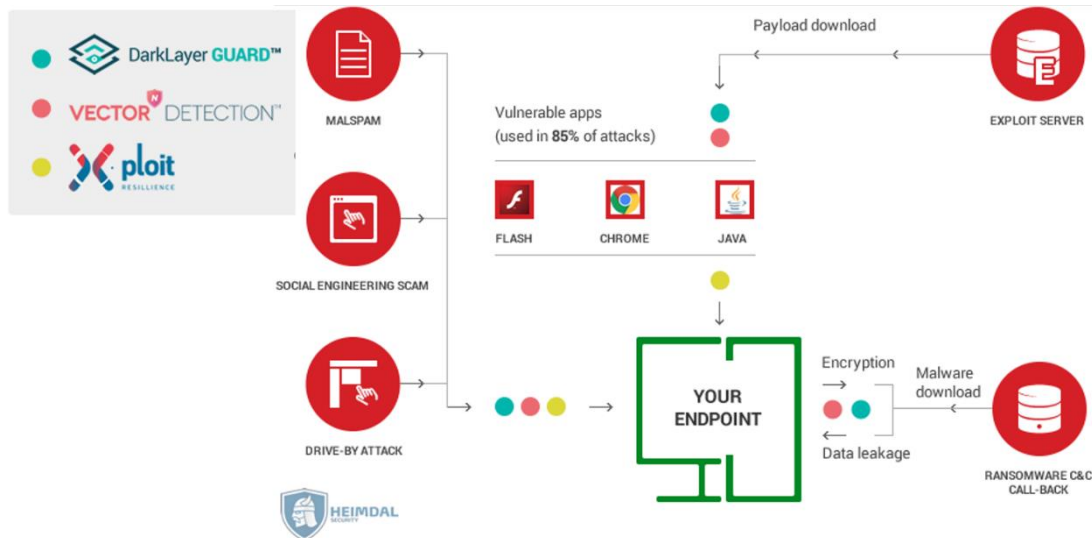
Why add Darklayer Guard™ to my Endpoints ?

By exploiting code and using trusted software criminals can easily bypass Antivirus, Behavior and Code Scanners, as well as Firewalls.

Using 2-way Device-to-infrastructure traffic scanning and our unique infrastructure intelligence, Darklayer Guard™ can stop **Ransomware, APT's, Data-leaks** and **that no other solution can**. Combining this ability to block attacks, with our **TTPC technology**, enables administrators to spot attack processes quickly. Darklayer Guard™ is a great add-on for any security solution offering you **HIPS** capabilities.

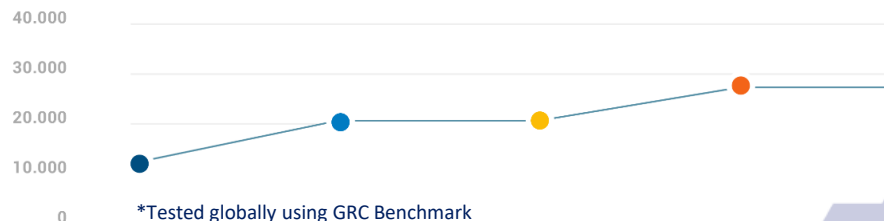
Superior speed and surgical accuracy

Using a self-learning technology combined with a small local database, our Darklayer Guard™ technology can almost always predict, if traffic is malicious, providing **enhanced speed* and security**. To enhance processing for unknown requests, Darklayer Guard™ uses Globally located cloud servers.

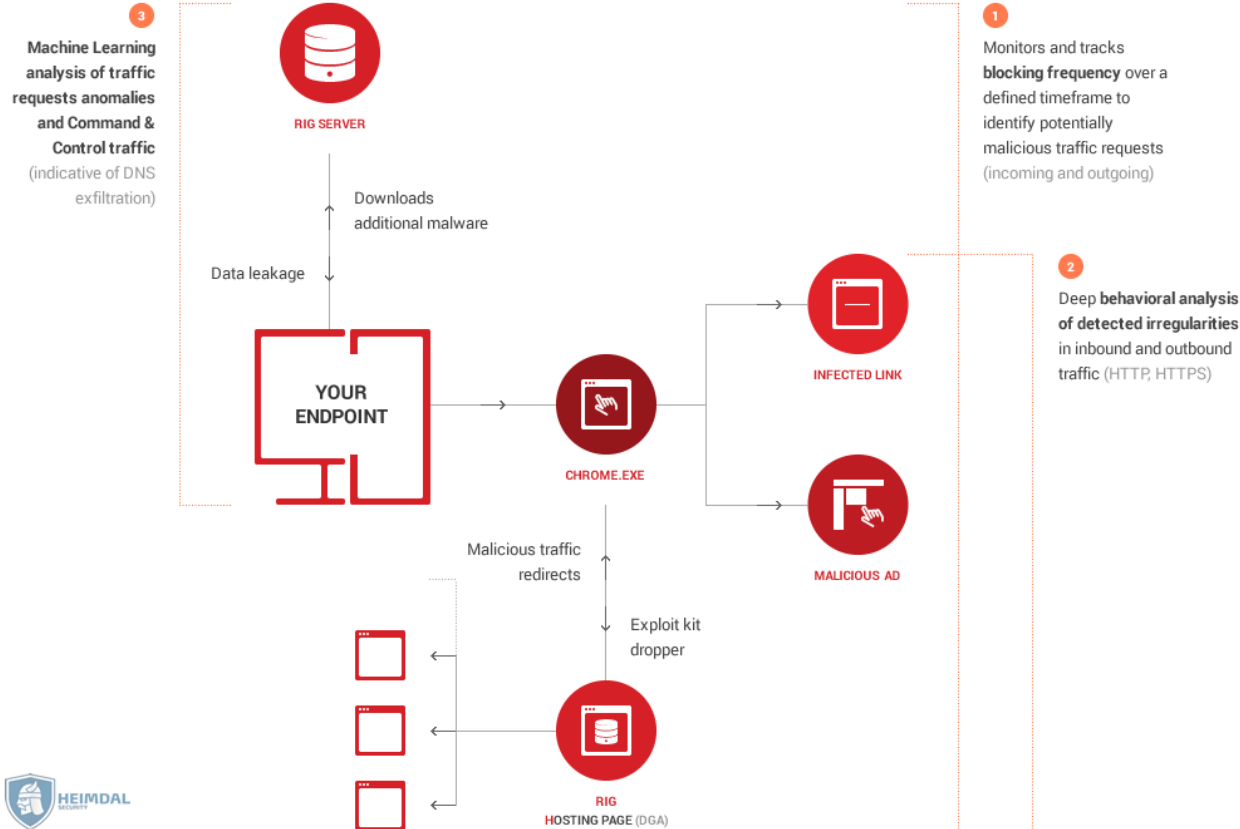


AVG. LATENCY OVER 1.000
REQUESTS 1 MS

Heimdal	NTT	Google	OpenDNS
0.011	0.020	0.020	0.028



4 **Threat to Process Correlation (TTPC)** - tracks device-to-malicious infrastructure communication and pinpoints the targeted process



Discover even hidden or dormant malware threats

Vector^N DetectionTM uses NO scanning of code and NO auditing of system processes. Using **Machine Learning Detection (MLD)** and **IOA/IOC's** this new technology will detect attacks at the **traffic layer**.

By tracking device-to-infrastructure communication and using a self-learning mechanism Vector^N DetectionTM will find malware that no Antivirus or Endpoint platform can detect.

Compliance and Vulnerability management

1. Automatic deployment/re-deployment of patches
2. Silent software installation and on-the-fly
3. Silent patching without user interruption
4. HTTPS transfers from Heimdal servers anywhere in the world
5. Covers both feature and security patches
6. Patch release to install time of less the 4 hours avg.
7. Configurable installs & patches – and how much to delay
8. Version management included
9. Offers installation catalogue, managed by the admin
10. Un-installation of software supported
11. Scheduling of updates according to PC clock

Advantages and Benefits

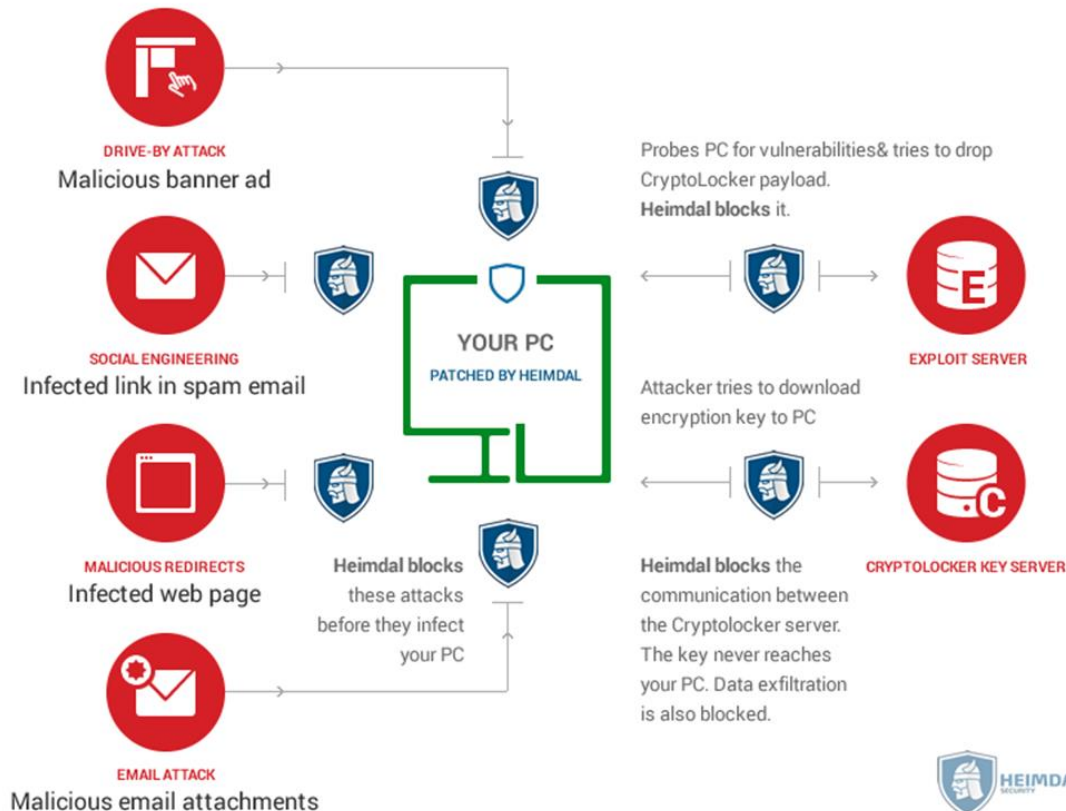
1. Less time used on checks – and always compliant
2. Less time spent on building images, packages and no reboots
3. Increased productivity and less time spent on support
4. Secure packages and updated machines – anytime/anywhere
5. Ensures you are always updated
6. Quick exploit kit protection and best possible compliance
7. Can be customized to fit your organization's needs
8. Full compatibility to legacy software
9. Enhances security by removing needs for local admin rights
10. Can remove unwanted software from your machines
11. Updates always fit to employees in their time zone



Foresight Ransomware protection



Types of ransomware: Cryptolocker, CryptoWall, TorrentLocker, TeslaCrypt, CTB-Locker, Locky.



Foresight offers 5-layers Ransomware Protection

Wannacry, CTB-Locker, Cryptolocker, or Cryptowall is likely the most advanced malware in the world.

Heimdal offers protection where antivirus products give up - offering Attack blocking, Patching, Exploit blocking, Dropper protection or key delivery filtering.

Infections can happen either via vulnerabilities or via exploits delivered from legitimate website banners and go undetected by antivirus. Once the exploits are executed, Malware droppers deliver the payload, which can avoid your antivirus. By doing so hackers bypass traditional endpoint protection.

Heimdal uses the 5-layers to stop Ransomware attacks at different levels.





Antivirus using Signature, Code and Behavior scanning to detect and remediate

Viruses

APT's

Financial Fraud

Data leaks

Ransomware

Remediation with minimal effort!

Thor Vigilance

(X-Gen Antivirus + EDR)



Independent Tests of
Anti-Virus Software

100,00% Detection*

Offering market leading Next-Gen Antivirus capabilities **Thor Vigilance** will detect and mitigate even next-gen threats. Using all the techniques known by both traditional and next-gen antivirus engines Thor Vigilance offers market leading detection and mitigation.

* AV-Comparatives.org Malware Protection Test – Feb 2018

Local File/Signature & Registry scanning

Thor Vigilance uses real-time **low impact** in-memory and file and signature scanning, combined with active registry change scanning to provide leading edge traditional type Antivirus detection and mitigation.

Real-Time Cloud Scanning

All files not-known to the local database are sent to our cloud for scanning. Using 1.000 CPU cores topped with **Machine Learning Detection** algorithms, we add another dimension to detection.

Sandbox and backdoor inspection

Files that still do not show as malware, enter our **sandbox** to see if they act as malware. This is done by also checking the file communication to see if it tries to contact **Command and Control servers**.

Process Behavior based scanning

When files start to execute Thor Vigilance continues to monitor processes and process changes with Heuristic, **Behavior engines** to give our X-Gen Antivirus the ability to detect code changes at all levels.

Thor Vigilance

(X-Gen Antivirus + EDR)



Preventing the unknown and catching the known.

Combine Thor Foresight and Thor Vigilance to give you proactive IOC's and enhanced IOA's.
Thor Foresight enriches our Thor Vigilance X-Gen Antivirus, with a unique EDR ability,
to mitigate even concealed or unknown samples.

Thor Foresight

Unique threat prevention and unique traffic based detection of hidden or unknown malware samples, Thor Foresight delivers unique EDR **IOA/IOC** intelligence to Thor Vigilance

Thor Vigilance


It leads the field in **malware detection** testing on its own, but when supplied with the Thor Foresight IOA/IOC intelligence, Thor Vigilance will be able to **mitigate** otherwise hidden threats



Thor Vigilance

(X-Gen Antivirus + EDR)





28 Scanned files

7 Infections found

53% Infection

VIGILANCE

Search

HOSTNAME

Q

LATEST INFECTIONS VIEW | INFECTIONS TYPE VIEW | HOSTNAME/INFECTIONS VIEW | QUARANTINE

A TOTAL OF 56 LISTINGS

DOWNLOAD CSV

HOSTNAME	STATUS	INFECTION NAME	THREAT CATEGORY	INFO	TIMESTAMP
<div><input checked="" type="checkbox"/> Select all</div> <div><input checked="" type="checkbox"/> QUARANTINE</div> <div><input checked="" type="checkbox"/> DENY ACCESS</div> <div><input checked="" type="checkbox"/> WHITE LIST</div> <div><input checked="" type="checkbox"/> DELETE</div>					
<input checked="" type="checkbox"/>	LOREM IPSUM	LOREM IPSUM	LOREM IPSUM	LOREM IPSUM	02.10.2017 01:40:00
<input checked="" type="checkbox"/>	LOREM IPSUM	LOREM IPSUM	LOREM IPSUM	LOREM IPSUM	02.10.2017 01:40:00
<input checked="" type="checkbox"/>	LOREM IPSUM	LOREM IPSUM	LOREM IPSUM	LOREM IPSUM	02.10.2017 01:40:00
<input checked="" type="checkbox"/>	LOREM IPSUM	LOREM IPSUM	LOREM IPSUM	LOREM IPSUM	02.10.2017 01:40:00
<input checked="" type="checkbox"/>	LOREM IPSUM	LOREM IPSUM	LOREM IPSUM	LOREM IPSUM	02.10.2017 01:40:00
<input checked="" type="checkbox"/>	LOREM IPSUM	LOREM IPSUM	LOREM IPSUM	LOREM IPSUM	02.10.2017 01:40:00
<input checked="" type="checkbox"/>	LOREM IPSUM	LOREM IPSUM	LOREM IPSUM	LOREM IPSUM	02.10.2017 01:40:00
<input checked="" type="checkbox"/>	LOREM IPSUM	LOREM IPSUM	LOREM IPSUM	LOREM IPSUM	02.10.2017 01:40:00
<input checked="" type="checkbox"/>	LOREM IPSUM	LOREM IPSUM	LOREM IPSUM	LOREM IPSUM	02.10.2017 01:40:00
<input checked="" type="checkbox"/>	LOREM IPSUM	LOREM IPSUM	LOREM IPSUM	LOREM IPSUM	02.10.2017 01:40:00
<input checked="" type="checkbox"/>	LOREM IPSUM	LOREM IPSUM	LOREM IPSUM	LOREM IPSUM	02.10.2017 01:40:00

FIRST PAGE

1

2

3

...

9

LAST PAGE

GO TO PAGE

123

ITEMS PER PAGE

10

Thor Vigilance EDR and management features

The Thor Vigilance suite offers a effective overview of threats, combined with easy to use, but advanced remote remediation features in a single interface management for your antivirus, enabling you to remotely execute a number of tasks such as.

- Differentiated Group Policy settings
- Scheduling of scans per group
- **Remote quick scan** per device or per group
- **Remote full scan** per device or per group
- Remote delete per device or per group
- **Quarantine of TTPC processes (With Foresight)**
- Exclusion from scan
- Quarantine of selected processes.

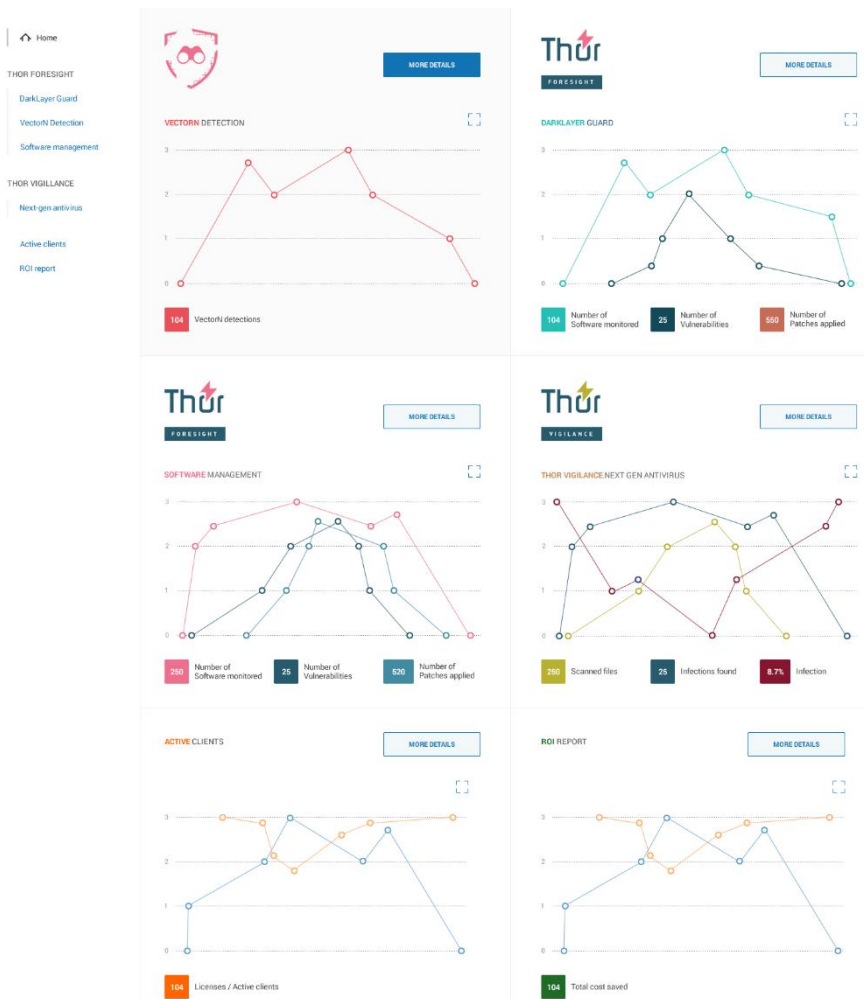
Thor Vigilance combined with Thor Foresight, also gives **EDR features** such as:

- User compromise
- Process exploits
- Malware undetectable by Antivirus

Unified Threat Platform



Unified Threat Dashboard



Heimdal UTD (Optional API for SIEM)

Heimdal Corporate offers real-time threat and status reporting, delivered in intervals of your choosing. Data is graphed and scaled daily, weekly or monthly and can be integrated into SIEM via API.

The Heimdal UTD stores the **entire history** as long as you are a customer and will help you perform compliance audits and risk assessments.

Coupled with weekly reports, data exports, e-mail alerts and data drill down built-in, Heimdal UTD offers a powerful and simple way to manage your environment.

Heimdal Corporate UTD helps you do:

- Next-Gen malware** prevention, with HIPS (DarkLayer Guard)
- Data leakage** prevention and **Forensics** (DarkLayer Guard)
- Quick response** to hidden threats (TTPC)
- Hidden threat detection**, with HIDS for what AV can't see (VectorN)
- Vulnerability** management and compliance (X-ploit resilience)
- Automated and Enhanced **Threat Mitigation** (Next-Gen AV)
- Lifetime history storage** for auditing and compliance

Easy policy creation and deployment



Home

THOR FORESIGHT

- DarkLayer Guard
- VectorN Detection
- Software management

THOR VIGILANCE

- Next-gen antivirus
- Active clients
- ROI report

Back to Group policies

Test 1

General

Thor Vigilance

Thor Foresight

Darklayer Guard

VectorN detection

Software management

☒ Enable software management

MANAGE APPLICATIONS | 38 APPS |

INSTALL ALL <input type="checkbox"/>	UPDATE ALL <input checked="" type="checkbox"/>	ALLOW INSTALL <input type="checkbox"/>	APPLICATIONS	DELAY <input type="checkbox"/>	VERSION
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	7-zip x86	2 Days <input type="checkbox"/>	16.02.00.0 <input type="checkbox"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Adobe Acrobat Reader DC	4 Days <input type="checkbox"/>	Latest version <input type="checkbox"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Adobe Flash Player 20 ActiveX	5 Days <input type="checkbox"/>	Latest version <input type="checkbox"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Adobe AIR	5 Days <input type="checkbox"/>	Latest version <input type="checkbox"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Adobe Flash Player 20 NPAPI	6 Days <input type="checkbox"/>	Latest version <input type="checkbox"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Adobe Reader	7 Days <input type="checkbox"/>	Latest version <input type="checkbox"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Adobe Shockwave	7 Days <input type="checkbox"/>	Latest version <input type="checkbox"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	CCleaner x64	7 Days <input type="checkbox"/>	Latest version <input type="checkbox"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Chrome	8 Days <input type="checkbox"/>	Latest version <input type="checkbox"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Classic Shell x32	9 Days <input type="checkbox"/>	Latest version <input type="checkbox"/>

CHECK INTERVAL | 1 MIN |

APPLICATIONS BLACKLIST 1

ADD NEW APP TO UNINSTALL QUEUE

Firefox Starting with this word ☐ ADD

Group Policies and Active Directory integration

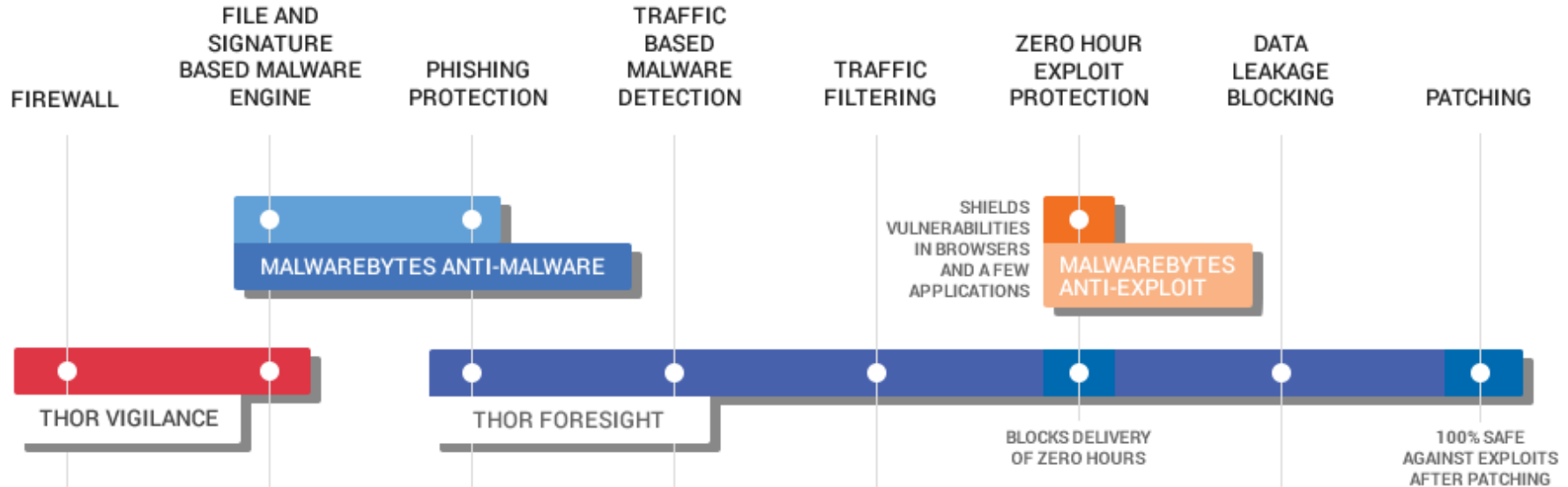
Heimdal UTD allows you to **define policies** for each component in detail – DARKLayer Guard, VectorN Detection and X-ploit Resilience. You can also do whitelisting and blacklisting of websites per active directory group of your Heimdal environment and even custom blocking pages per active directory group.

This gives you a powerful option to individually tailor your entire IT environment and create policies, which applies to **your exact needs** across the Active Directory groups in the organization.

Once configured Heimdal deployment is simple and easy and can happen through any MSI deployment tool.

Thor Premium vs. Malwarebytes

For internal training only



Hemidal Thor Foresight – malware prevention

Heimdal Thor Foresight offers module capabilities which are not featured at all, or only partly featured in the Malwarebytes packages. Offering full patching and attack filtering capabilities the Thor Foresight product overshadows the limited proactive features of Malwarebytes obsolete.

Heimdal Thor Vigilance – reactive head to head

In reality Malwarebytes is a Antivirus replacement, but strong in PUA (Potentially unwanted application). In a malware detection comparison Thor Vigilance will be superior, using File and Signature, Heuristic, Behavior, Cloud based and Sandboxing techniques

Width beats it all – Thor Premium

Looking at the width, the Thor Premium package offers patching, exploit mitigation, DNS/HTTP/HTTPS filtering, Antivirus detection at all levels, data leakage protection and a firewall – which makes it a far superior prevention and detection package to Malwarebytes.

Idaho State Department of Agriculture prevents exploits with Thor Foresight

Interview with Raffaele Dore, IT-Manager. “Because the level and number of threats present has been increasing, we decided it was time to implement an extra layer of protection that wasn’t too intrusive and yet effective, and that wouldn’t interfere with our endpoint protection suite. Several of our employee’s’ job requires them searching and exchanging information online, which makes them vulnerable to phishing websites, watering hole and drive-by attacks. We were looking for a product specializing in detection and prevention of such malware.”

What problem did Heimdal THOR Foresight solve for you?

Our endpoints are often the target of drive-by attacks. Heimdal has proven to be very effective at blocking them.

Could you tell us in your view how Heimdal THOR Foresight stopped a ransomware or phishing attack?

Our agency is the constant target of phishing and spear-phishing campaigns. Heimdal has helped us with the detection and mitigation of various exploits and malware from infecting our network.

What key aspects did Heimdal THOR Foresight help you improve or change in your company?

Heimdal’s detailed reporting has helped us detect which kind of threats we are most exposed to and apply proper countermeasures.

If you were to recommend Heimdal THOR Foresight to others, what would you tell them?

Nowadays is every easy to stumble across compromised websites, laced with malware and exploits ready to deploy into one’s system. Heimdal is the answer to these online threats; it is a very effective shield against a wide range of malicious content that constantly lurks the net.

Get in touch at:
contact@heimdalsecurity.com



Heard County frees up resources and time.

Interview with Andrew Williams from Heard County, Georgia. The County has used Heimdal Thor Foresight for almost a year and shares their experience with the solution and Foresights's positive impact on the organization.

We started learning about Heimdal by reading the Heimdal blog and found it to be quite informative and very educational. After also reading some of their threat alerts we decided to look further into the Heimdal product.

What is especially interesting about Heimdal – and how does it provide you with added value?

"Running software updates across our systems has always been a headache for us. Since this is a key route for keeping cybercriminals out, we had to do something and we were surprised about the value:

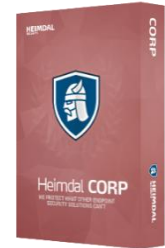
- The automatic update system just works automatically and seamlessly and I was surprised, because doing updates can be tricky.
- and just recently we also discovered the threat filtering system and keeps finding threats we weren't even aware that we had.

Using Heimdal to solve our challenge, regarding vulnerabilities, is especially related to web plugins, but Heimdal has proved really effective in maintaining any third party applications. The ease of use is phenomenal and once it is set, it just goes by itself. Amazing time saver, without a doubt. Keeping software up-to-date is a breeze for a change. With the threat filtering now also in place, we can see how much our Antivirus and perimeter firewall systems are actually missing out. And the fact that Heimdal works anywhere you go – is just great.

Can you recommend Heimdal Security to others?

"Most certainly! We are very happy with the solution. Not just the software itself, but also Heimdal Security as a company. They always keep an open line with us, communicating constantly, and they are very knowledgeable. They always have a strong recommendation from our part!"

Get in touch at:
contact@heimdalsecurity.com



Boreal Transport chooses Thor Foresight for simpler patch management

Interview with Kjell Magnus Hernar, IT Coordinator at Boreal Transport. The Company purchased Heimdal and shared their experience with the solution and Heimdal's positive impact on the organization.

"We found Heimdal online and thought of it as being a simple and straight forward alternative to handling software updates through SCCM.

We tried Heimdal in a POC period and were very satisfied with how simple it really is to use."

What is especially interesting about Heimdal – and how does it provide you with added value?

"Heimdal is very simple to setup and very simple to use. We use Heimdal for both installing and updating software. We thought we would only do software updating with Heimdal, but we are now also using it for complete 3rd party application software management.

On top of this we also got additional value in the fact that we can use Heimdal in protecting against Ransomware, Trojans and other threats.

We had a small issue during the implementation of the Heimdal filtering, but the support has been great and very helpful, whenever we have had the need for them.

Heimdal is also constantly evolving the solution and adding more features at no extra cost to us.

Can you recommend Heimdal Security to others?

"Yes, most certainly. Heimdal is a great solution for any company and their support and follow up is great."

Get in touch at:
contact@heimdalsecurity.com



Donegal County Council Takes the security of its data very seriously.

**Interview with Sean Dunnion,
Project Leader, Information Systems,
Donegal County Council**

In light of current cyber threats – ransomware in particular – and their many ramifications, Donegal made the decision to add an additional layer of security to their current protection.

Donegal explored a number of various solutions and, after evaluating them, identified Heimdal as the best solution for them. After a successful proof of concept, Heimdal CORP was selected and pushed out across 900 endpoints.

Solution provided

Heimdal Thor Foresight was installed on all the endpoints used in the Donegal County Council. The installation was simple: it only entailed downloading an MSI file from the Heimdal dashboard and rolling it out via GPO.

As a result, the Country Council can now monitor the Traffic Overview for each endpoint, can automate Patch Management for the top 40 security-critical applications, and enjoy the Advanced Malware Engine and Reporting – all through a simple, user-friendly Unified Threat Dashboard.

Consequently, they can prevent infections from taking over the network and can mitigate risks before they turn into fully-blown cyber-attacks.

Why Heimdal

“The main reason we went for Heimdal is that it offered another layer of security (patch management and traffic monitoring/blocking at the network interface level) for us to counter-act the very real and numerous threats of Ransomware that are out there at the moment”.

Get in touch at:

contact@heimdalsecurity.com



COMHAIRLE CHONTAE

Dhún na nGall

DONEGAL COUNTY COUNCIL

Cottingham & Butler selects Heimdal for next-gen prevention

Being a key player in the United States insurance brokerage industry, Cottingham & Butler has a high focus on IT security, keeping both customer and internal data secure.

“Protecting the confidentiality, integrity, availability of systems and data is crucial, both because our clients have put their trust in us and to protect our brand.

Being a top 40 insurance broker in the United States, we need to maintain the highest standards”, says Phil Niles, VP of Information Technology.

Heimdal for next-gen

As part of the aspiration to constantly improve security, Cottingham & Butler was looking for a next-generation protection product to add another layer of security as part of their defense-in-depth strategy.

The choice ended up being Heimdal Security.

What is especially interesting about Heimdal – and how does it provide you with added value?

“Being proactive about our IT security has always been a challenge”, says Niles. Heimdal adds clear value in the fact that it is very proactive

- The automatic update system works on the fly without any reboots, and it updates faster than some other protection products we have.
- In terms of preventing attacks, we have already seen a clear value in the first couple of months that we have used Heimdal.
- One of our core concerns is, of course, that we also want to use Heimdal proactively against Ransomware

Challenge handling

We did have a challenge with Heimdal conflicting initially with another of our security products. After a Teamviewer

session with their support and development team – and about 2 months’ development time, Heimdal had brought out a new version that solved the problem and made sure that our security solutions were fully compatible.

Can you recommend Heimdal Security to others?

“Absolutely. Heimdal is a flexible company and a fast way to improve our security. It helps us prevent attacks before they even happen.”



Cottingham & Butler

C&B Insurance | SISCO | HealthCorp | Safety Management

Get in touch at:
contact@heimdalsecurity.com



HEIMDAL SECURITY IN THE MEDIA

FORBES - <http://www.forbes.com/sites/stevemorgan/2016/01/02/one-million-cybersecurity-job-openings-in-2016/#31f324b07d27>

BUSINESS INSIDER - <http://uk.businessinsider.com/ransomware-cryptmix-promises-to-pay-ransoms-to-charity-extortion-virus-2016-5>

THE GUARDIAN - <https://www.theguardian.com/technology/2014/jun/04/cryptolocker-ransomware-uk-police-action>

THE VERGE - <http://www.theverge.com/2016/2/16/11016280/android-virus-malware-mazar-heimdal-denmark>

THE NEXT WEB - <http://thenextweb.com/apps/2016/02/16/android-malware-that-can-erase-devices-remotely-being-used-in-attacks/>

DIGITAL TRENDS - <http://www.digitaltrends.com/mobile/mazar-android-malware-news/>

HUFFINGTON POST - http://www.huffingtonpost.co.uk/2016/02/18/mazar-sms-virus-can-hands-over-controll-of-an-android-smartphone-to-hackers_n_9263238.html

PC MAG - <http://www.pcmag.com/article2/0,2817,2499360,00.asp>

ARS TECHNICA - <http://arstechnica.com/security/2015/12/newest-ransomware-pilfers-passwords-before-encrypting-gigabytes-of-data/>

INFOSECURITY MAGAZINE - <http://www.infosecurity-magazine.com/news/rig-ek-ramps-up-to-spread-cryptmic/>

THE INQUIRER - <http://www.theinquirer.net/inquirer/news/2435483/banking-trojan-dyreza-is-targeting-windows-10-and-microsoft-edge-users>

SECURITY WEEK - <http://www.securityweek.com/cryptowall-40-released-filename-encryption-feature>

GRAHAM CLULEY - <https://www.grahamcluley.com/2016/05/ransomware-promises-donate-ransom-fees-childrens-charity/>

SOFTPEDIA - <http://news.softpedia.com/news/malvertising-campaign-using-rig-ek-detected-pushing-crypmic-ransomware-508475.shtml>

DARK READING - <http://www.darkreading.com/attacks-breaches/cryptowall-40-spreading-via-angler-drive-by-download-campaign/d/d-id/1323380>

SC MAGAZINE - <http://www.scmagazine.com/heimdal-security-outlines-drindex-malware-attack/article/423464/>

HEISE.DE - <http://www.heise.de/security/meldung/Erpresser-ruesten-nach-Verschluesselungs-Trojaner-TeslaCrypt-4-0-gesichtet-3145559.html>

TECH REPUBLIC - <http://www.techrepublic.com/article/how-to-mitigate-ransomware-ddos-attacks-and-other-cyber-extortion-threats/>

THE REGISTER - http://www.theregister.co.uk/2016/08/12/banking_trojan_scylex_ad/

HACK READ - <https://www.hackread.com/no-more-ransom-anti-ransomware-portal/>

BETA NEWS - <http://betanews.com/2016/07/18/stampedo-ransomware/>

THREATPOST - <https://threatpost.com/adwind-rat-resurfaces-targeting-danish-companies/119060/>

Any Questions?

Farokh Karani

Sales Director – North America at Heimdal™

Email: fka@heimdalsecurity.com

Website: heimdalsecurity.com
