cythereal
TARGETING TARGETED ATTACKS

www.cythereal.com
info@cythereal.com

MAGIC™: Malware Genomic Correlation System

Changing The Rules Of **Cyber Engagement**

Hunting Malware With Malware

Cythereal MAGIC™ is a transformative anti-malware technology that is rewriting the rules for hunting zero-day malware.
Instead of spending hours chasing IoCs to catch variants, analysts can generate bytecode based YARA rules within minutes and start hunting.

What MAGIC™ Does

- Identifies malware campaigns in malware collections
- Develops a profile of the attackers from the campaigns
- Detects targeted malware attacks across time and space
- Assesses the ability of a campaign to defeat an anti-virus system
- Generates YARA rules to hunt targeted malware attacks

How MAGIC™ Works

- Automatically unpacks malware to extract its payload
- Deobfuscates malware and extracts its genome
- Identifies malicious code techniques in genome
- Performs machine learning using code techniques, not IoCs
- Uses Abstract Symbolic Automata to construct YARA rules

Why Use MAGIC™

Improve the effectiveness of SOC in performing malware investigations.
Defend against zero-day malware attacks that target only your organization.
Get more out of existing investments in Anti-Virus, IDS, and EDR technologies.

Founded on Rigorous Research

Result of 10+ years research sponsored by US DARPA and other agencies

Independently Verified

Accuracy verified by US DoD agencies and Anti-malware companies

Highly Scalable

Elastic-cloud architecture, scalable to process 100K+ malware a day

cythereal
TARGETING TARGETED ATTACKS

www.cythereal.com
info@cythereal.com

MAGIC™ Early Warning System (EWS)

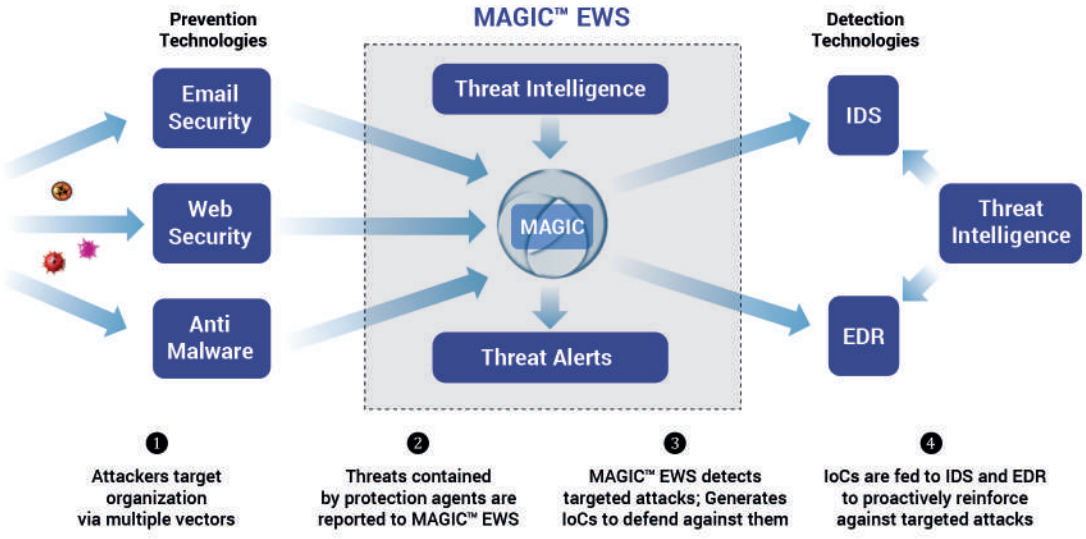
"A **Targeted Attack** is a threat in which threat actors *actively pursue* and compromise a *target* entity's infrastructure while maintaining anonymity. These attackers have a certain level of expertise and have sufficient resources to conduct their schemes over *a long-term period*. They can adapt, adjust, or improve their attacks to counter their victim's defenses."
Trend Micro

What MAGIC EWS does?

Most prevention technologies cannot withstand a targeted attack by an advanced adversary. MAGIC EWS hardens an organization's existing security infrastructure against such attacks by learning directly from an adversary's unsuccessful attempts. Instead of relying on stale threat intelligence of questionable relevance from third-parties, MAGIC EWS uses the organization's prevention technologies as the source of current and contextual intelligence. It continuously and automatically analyzes attacks stopped by these technologies to identify and track malware campaigns that are persistent, multi-prong, and escalating. For such pernicious campaigns it generates IoCs that may be used to prevent an attack from succeeding or contain them if already successful.

How it works?

Even the most well-resourced threat actor reuses proven malware code over multiple campaigns. MAGIC EWS leverages the sharing of code between malware to track and counter threats. Working in concert with an organization's email security, web security, and anti-malware, MAGIC EWS analyzes malware used in attacking an organization and identifies campaigns that are persistent and have a high likelihood of evading protection technologies. Further, MAGIC EWS automatically creates YARA rules using shared code and scours threat exchanges to get associated IoCs. The YARA rules and IoCs are fed into the intrusion detection and breach detection technologies to strengthen them with more relevant and contextual IoCs.



What is the value?

- MAGIC EWS provides a rapid, systematic, and adaptive approach to detect, prevent, and contain targeted attacks.
- MAGIC EWS enables an enterprise do more with its security budget by automating the laborious task of malware analysis needed for threat hunting and incident response.
- MAGIC EWS serves as a force multiplier by improving the ROI of an organization's existing investments in prevention and detection technologies.

About Cythereal: Cythereal is an offensive cybersecurity company that predicts, tracks, and investigates zero-day malware attacks.

537 Cajundome Blvd, Suite 111, Lafayette, LA 70506, USA • +1 (337) 781-8376