xorlab



REDEFINING ENTERPRISE EMAIL SECURITY

Spinoff ETH zürich

swiss made software

Email is attack surface. Manage it.

94% of malware and 96% of social attacks are delivered via email.

Source: Verizon Data Breach Investigations Reports 2018 & 2019

Today's email attacks easily bypass legacy defense controls. Here is why:

Reason #1: They are unique.

No two malicious emails are identical. Cyber criminals leverage technology to craft individual messages that bypass sender-based reputation systems and signature-based gateways at scale.

Reason #2: They impersonate trusted parties.

Attackers take advantage of the trust people put in email relationships and impersonate them by leveraging email's poorly implemented forms of authentication. Existing email security systems fail to detect such impersonation attempts.

Reason #3: They're tailor-made and low volume.

Sophisticated attackers only target specific people in your organization and deliver them highly personalized content. Targeted malware and phishing attacks are low volume and easily go undetected.

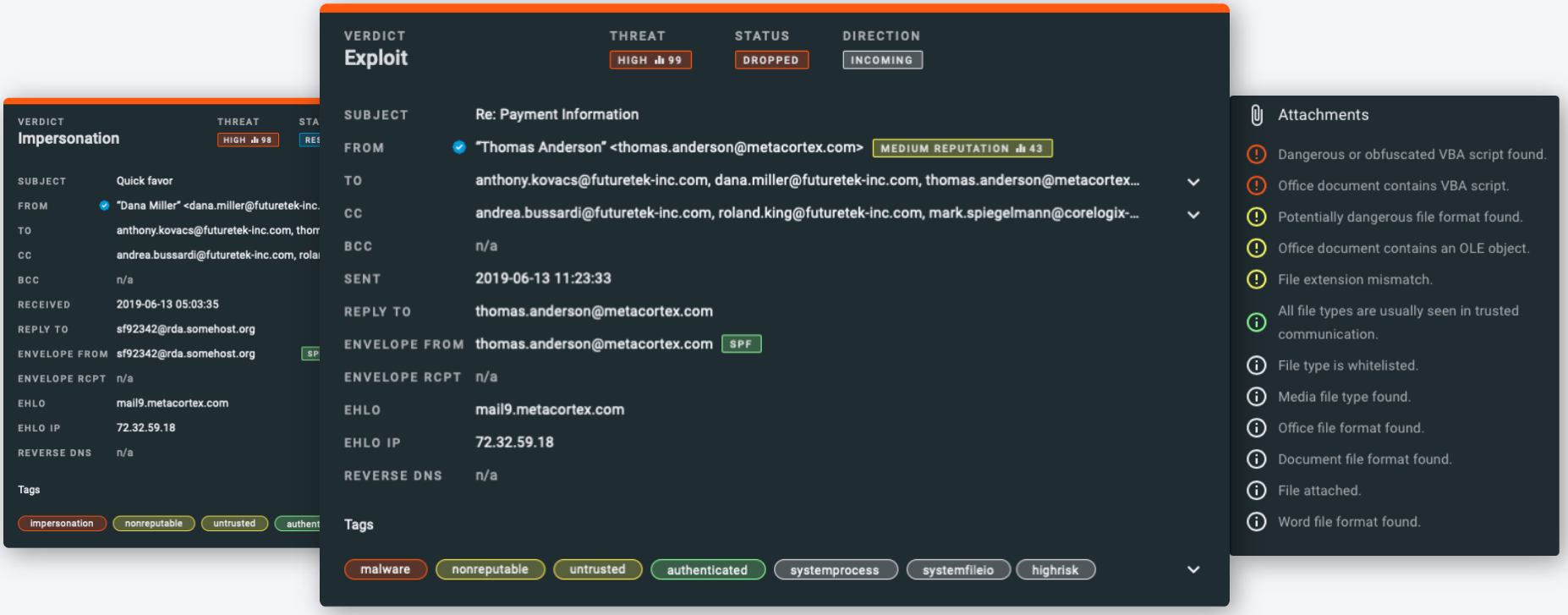
Reason #4: It's just words.

Many social-engineering attacks work without attachments or links. This lack in obvious risk indicators makes them invisible to existing security tools.

Enterprise email security redefined

xorlab's proactive email defense platform harnesses machine intelligence and advanced malware and zero-day exploit detection to protect your organization against the full range of targeted email attacks.

Packed with powerful automation and response tools, the platform enables your security operations teams to triage and respond to reported incidents quickly and proactively.



Product capabilities

Protect your organization, simplify your architecture and automate security operations with a proactive email security platform that integrates with Microsoft Office 365 and on-premise email infrastructures.

Inbound email protection

xorlab stops the full range of email attacks, with a strong focus on sophisticated targeted attacks and zero-day exploitation.

- Executive and employee impersonation
- Credential phishing and brand spoofing
- Ransomware, sabotage and industrial espionage

Email account compromise detection

xorlab analyzes hundreds of signals to detect compromised email accounts.

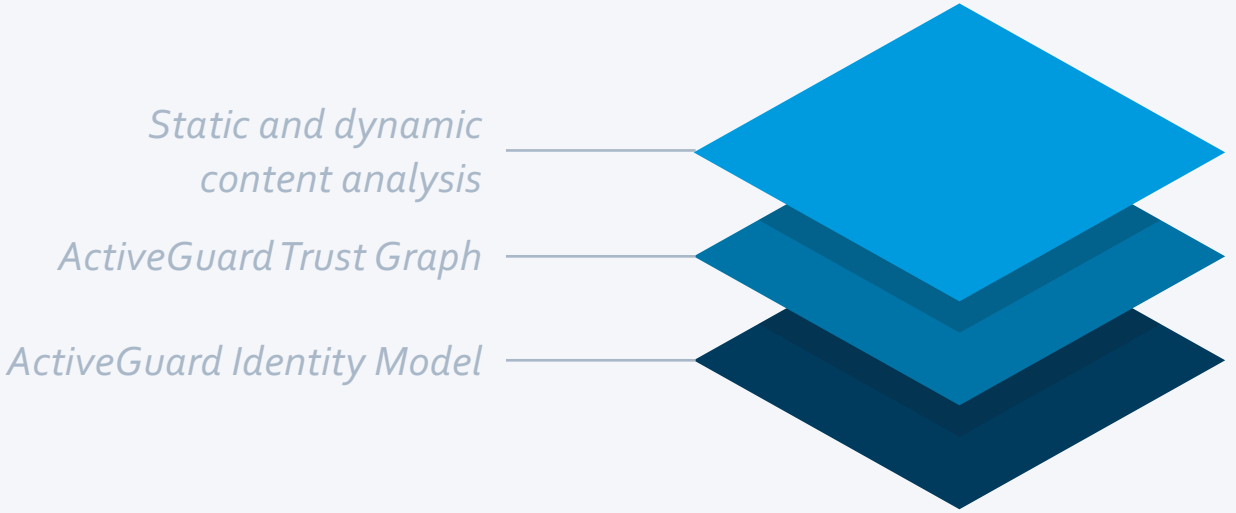
- Compromised employees
- Compromised suppliers and business partners
- Hacked external parties

SOC platform for email incident response and automation

Augment security operations teams with automation and tools to efficiently triage email incidents and respond to them quickly and proactively.

- Triage employee reported emails effectively
- Investigate and respond to critical incidents quickly
- Bulk remediate attacks across the entire organization

ActiveGuard Security Fabric



Static & dynamic analysis

Deep payload inspection, URL reputation monitoring and powerful, low-level software analysis allow accurate quantification of email attack surface.

ActiveGuard Trust Graph

Stateful encoding of internal and external communication patterns drives insights into type and strength of individual and organizational relationships.

ActiveGuard Identity Model

Accurate mapping of email addresses to known identities of employees, suppliers and external entities enables powerful analysis of behavior and relationships.

Your advantage with xorlab

Stop targeted attacks

xorlab's unique combination of machine intelligence and advanced exploit and zero-day protection capabilities enable detection of sophisticated email attacks. Even if the perpetrator is an authentic trusted party.

ActiveGuard Security Fabric

xorlab's threat detection fabric builds on proprietary models that understand local context, communication relationships and behavior, and leverages that understanding to make dynamic decisions based on the risk of every email it processes.

Automation and response tools

xorlab enables security teams in SOC and CSIRT to automate repetitive tasks, so that they can focus on fighting real threats. Threat analysis, triage and response complement existing defense capabilities to elevate email protection to the maximum security level.

Would you like to learn more?

Schedule a personalized product demo to see:

- Threat analytics, insights and reporting
- Automated triage, investigation and response tools
- Platform integrations into SIEM, SOAR
- and more of what ActiveGuard has to offer (your organization).

