

User Reported Phishing

How It Works – eBook



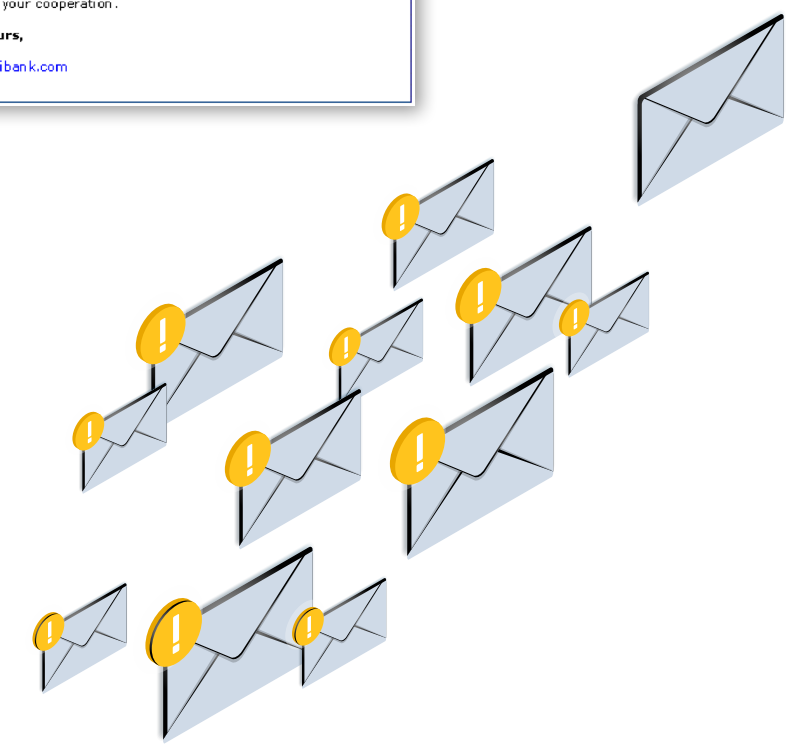
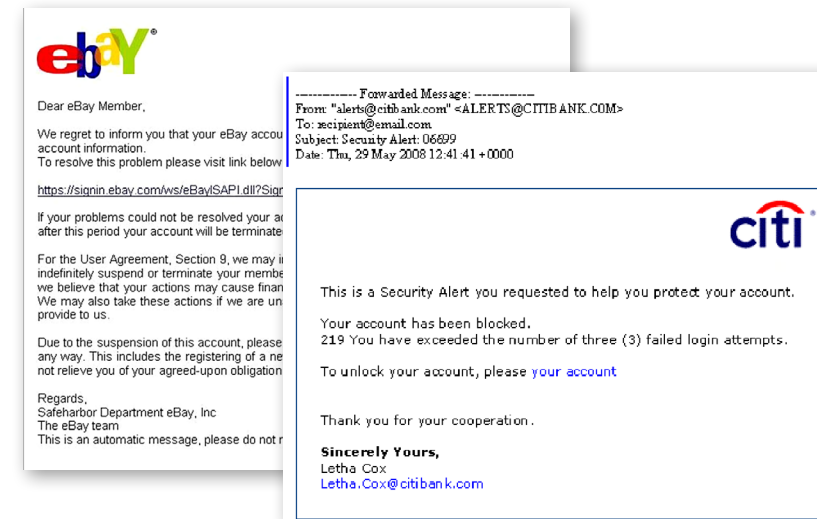
What is Phishing?



Phishing is a form of **social engineering** where attackers deceive people into revealing sensitive information (credential harvesting) or installing malware such as ransomware.

A major cause of corporate IT disruption stems from the **mail-borne delivery of advanced unknown malware**, phishing, and credential harvesting attacks.

There are approximately **15 billion SPAM and phishing emails traversing the internet everyday** and enterprise SPAM filters are working overtime.



Phishing Attacks Still #1 Attack Vector



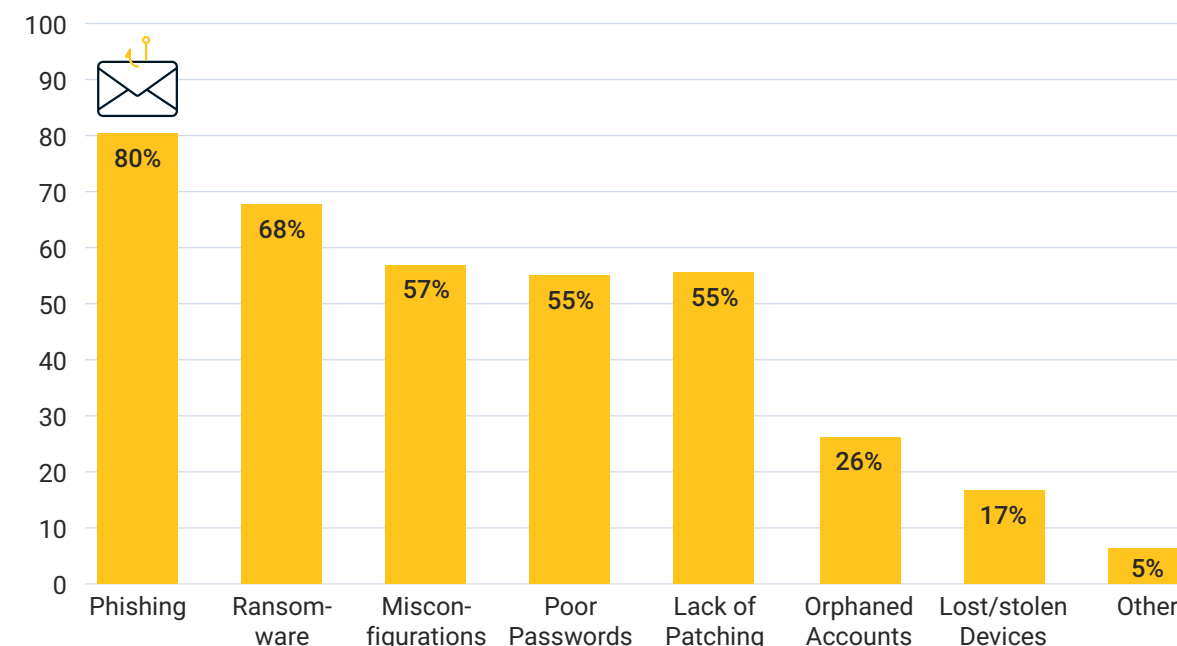
Even with the advances in heuristic analysis and phishing detection, email continues to be the most successful attack vector for both opportunistic and targeted-based attacks.

Recent studies show that **phishing attacks** continue to be **responsible for approximately 90% of data breaches**.

Advanced malware delivered by phishing emails has also become more sophisticated and evasive as it is engineered to avoid detection by perimeter email security and endpoint anti-malware solutions.

Common Security Concerns

What common security risk / entry points are you most concerned about?



Phishing is the most common security concern

Source: Fortra 2022 Pen Testing Report

Phishing Statistics By The Numbers



\$4.35M

**Average cost of a data breach
in 2022.**

Source: IBM

**Percentage of phishing attacks
targeting credential theft.**

58.1%

Source: Anti-phishing Work Group

Phishing Statistics By The Numbers



94%

Percentage of malware delivered via email

Source: Verizon DBIR 2021

50%

Percentage of people who fell for a phishing email because they were tired or distracted.

Source: Tessian

18-24

Age group that fell for phishing emails the most in 2022.

Source: Tessian

Advanced Phishing Attacks

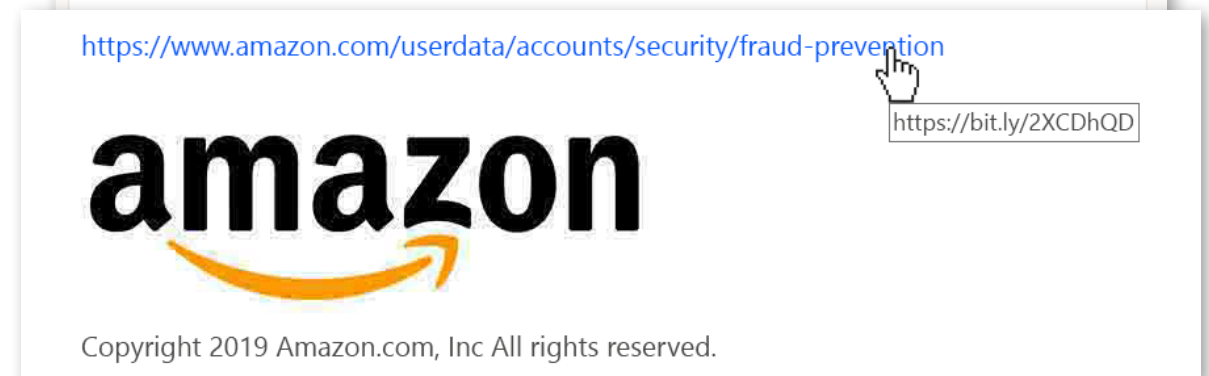
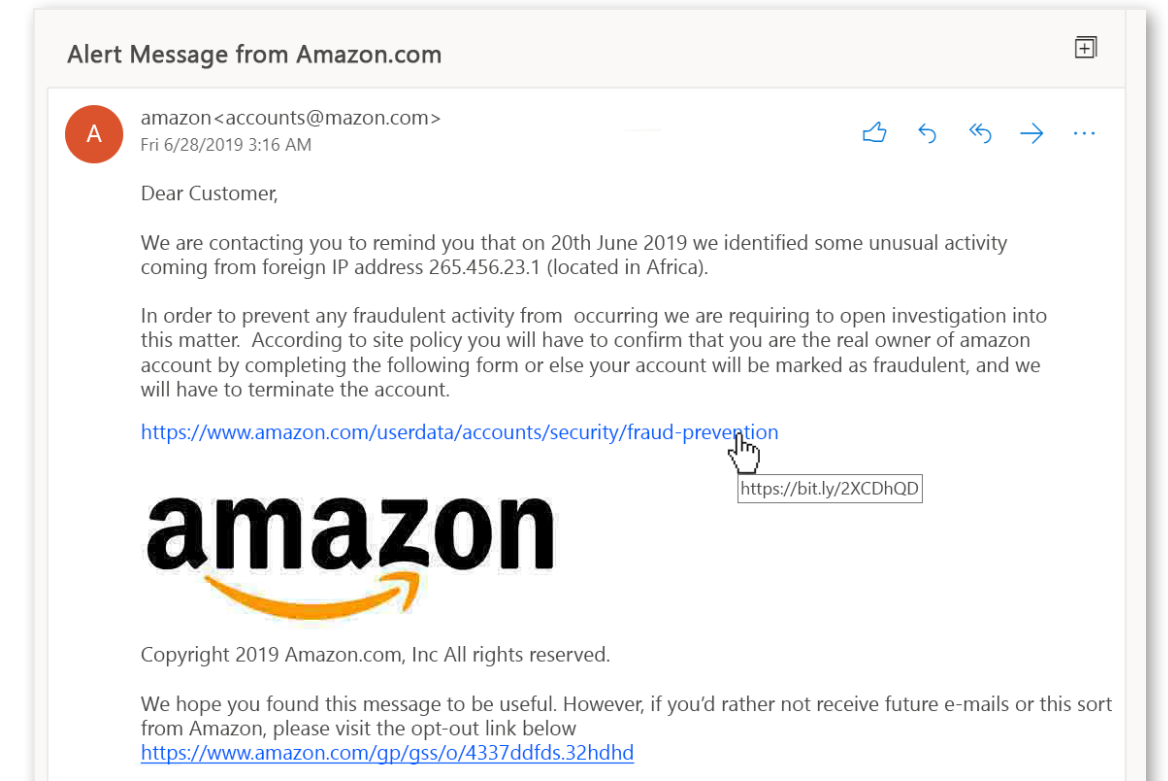


There are many different types of phishing attacks, but the most common attacks targeting the enterprise include:

Deception Phishing

Deception phishing is **one of the most common types of attack** and uses deception to **entice users into clicking a malicious link or downloading a file.**

Masquerading as a known brand, these opportunistic phishing emails leverage social engineering tactics sent blindly to a large audience. The links included often lead to cloned websites installing malicious code. Their success rate is typically low.



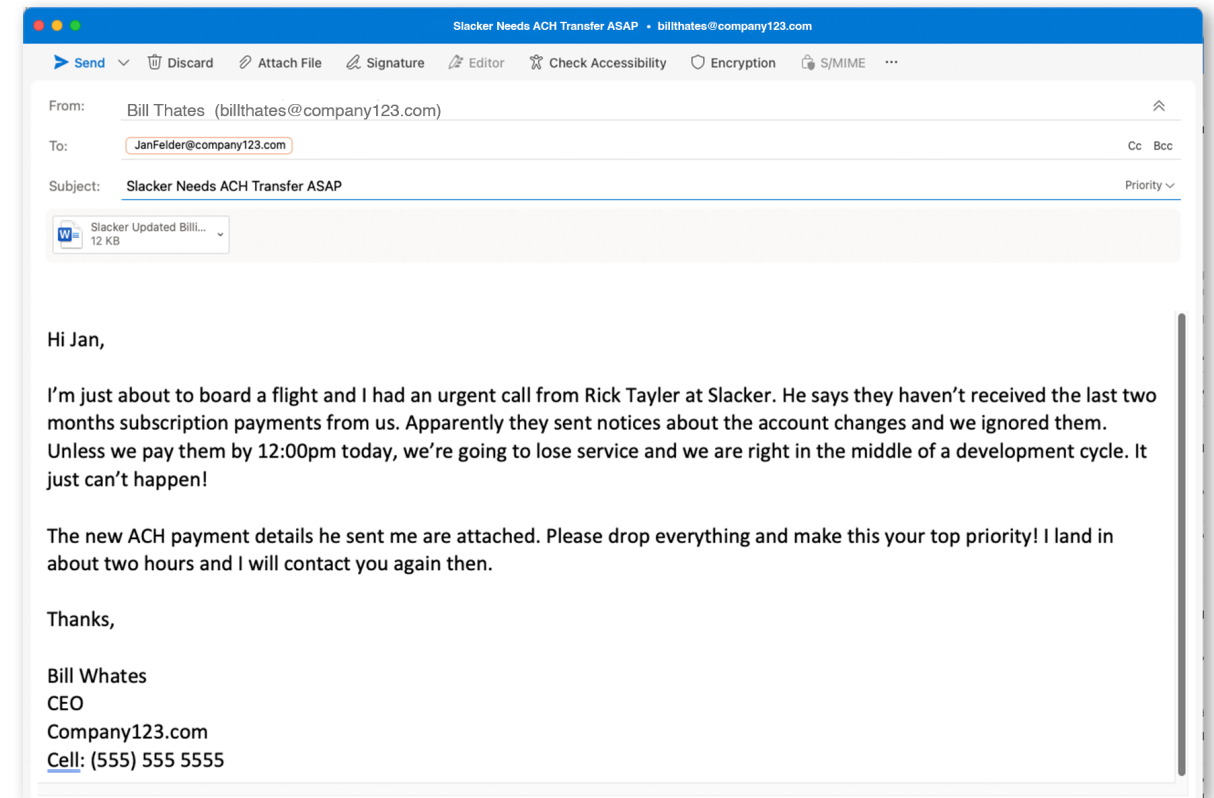
Advanced Phishing Attacks



Spear-Phishing & Whaling

A more targeted approach to email compromise is spear-phishing and whaling. Cybercriminals **gather publicly available information (OSINT) from multiple sources to target specific individuals within an organization.** Emails are crafted using real names or job functions to make the recipient believe the email originated from within the company or a trusted vendor.

Whaling attacks target high-profile or senior-level employees within an organization or masquerade as them to deceive others. In some cases, **bad actors may pose as the CEO to manipulate employees** into authorizing high-value wire transfers or a “zero hour” weaponized download link to malicious malware.



Because an email may appear to be from an internal or trusted source, the success of targeted phishing campaigns is much higher.

Advanced Phishing Attacks

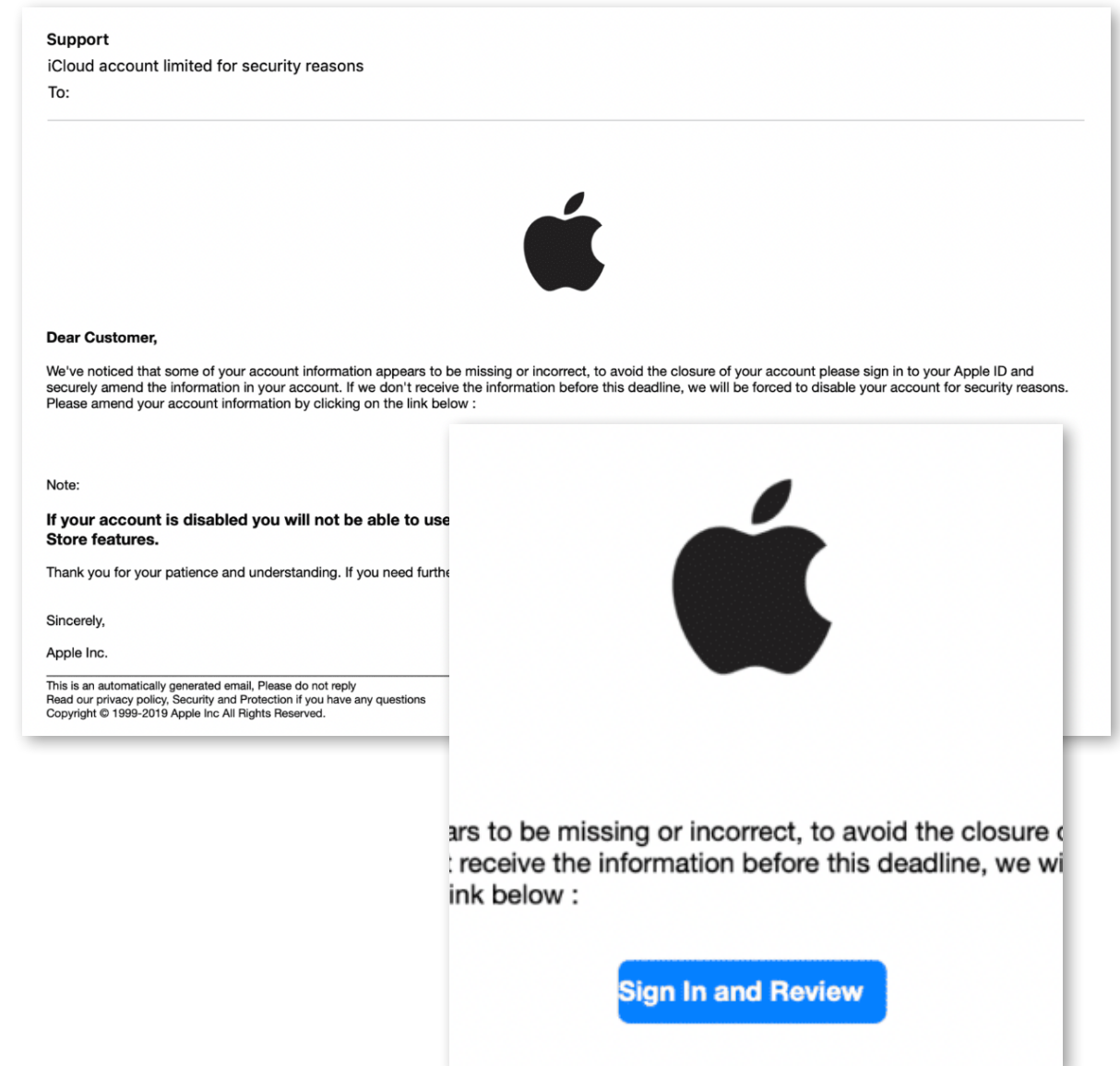


Credential Harvesting

Credential harvesting uses similar tactics to phishing attacks but focuses on **collecting specific account login and password information** to access financial systems.

58% of phishing emails are now credential harvesting attacks.

A common attack vector involves the **stolen credentials from vendors and other supply chain partners** to attack a target. The email directs targeted recipients to cloned websites from which the attackers harvest their login credentials. This often results in the unwanted pillaging of financial accounts and the selling of stolen confidential data.



Advanced Phishing Attacks

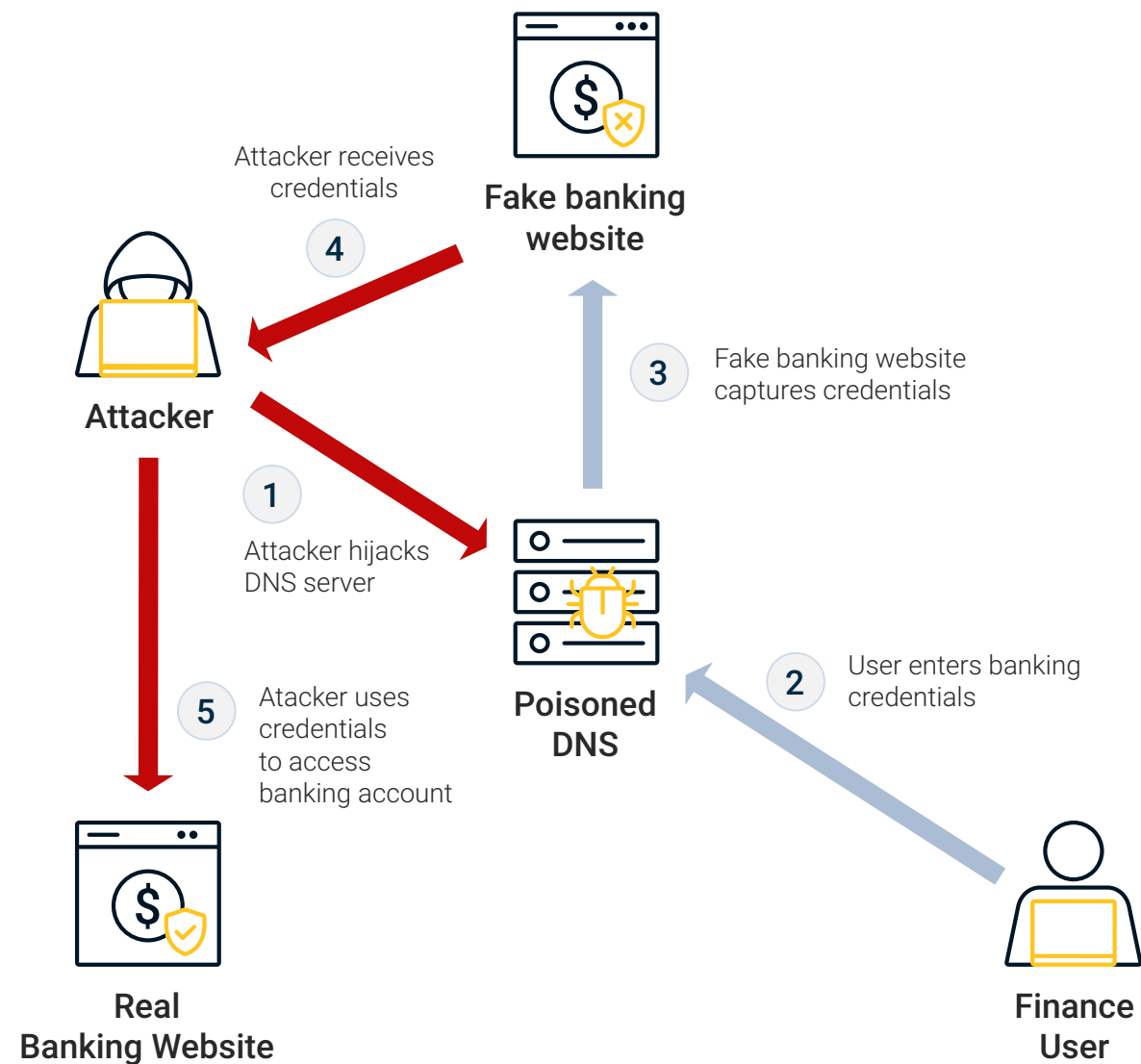


Pharming

Pharming involves **hijacking the user's browser settings or running a background process** that redirects users to a malicious site. Pharming attacks are often more difficult to detect.

The attacker's goal is to get financial data or harvest the user's credentials. Bad actors can also hijack a Domain Name Server (DNS) so that the **DNS server redirects a user to a cloned malicious website** rather than the website originally requested.

Pharmers often use phishing to infect a target system by **sending code via an email that the user clicks on**.



How VMRay Can Help...



User Reported Phishing

In larger Enterprises, MSSPs or MDR SOC's with hundreds of clients, the number of potential phishing emails reported by end-users to an Abuse Mailbox might reach hundreds daily. **Manual processing and triage of potentially malicious messages for further analysis can take up-to half an hour for a single email.**

Educating end-users on phishing attacks and how to identify them is a strategy that has gained widespread adoption in recent years. **The VMRay Abuse Mailbox enables SOC teams to create a dedicated mailbox with automated sandbox analysis.** This allows end-users to become part of the IT detection fabric and forward any "suspicious" emails missed by the company's perimeter-based SPAM/phishing solution for further analysis – without any SOC team intervention.



Detonation Required

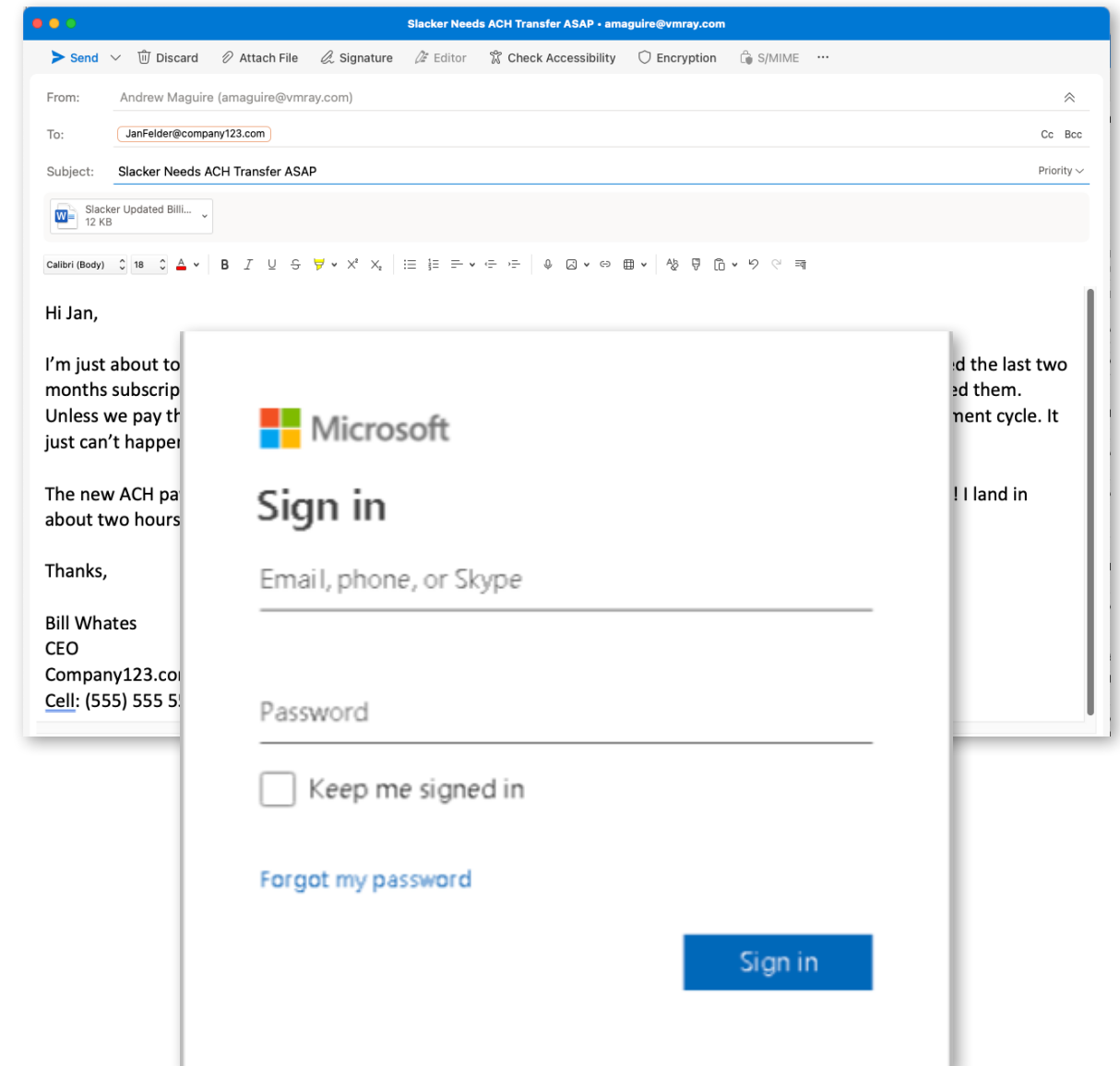
Currently, the only way to identify previously unknown, advanced phishing attacks is to **detonate them in a safe sandbox environment**, record the activity and analyze the results with machine learning for malicious behavior. If the malware payload suspect's it is in a monitoring environment used for analysis, it may withhold payload detonation to avoid detection – unless fooled into believing it's not.

Once the sample has passed through the analysis engine, post processing generates **noise-free reports with actionable intelligence**. The mapping of malicious sample characteristics to the industry-standard MITRE ATT&CK framework, proprietary VMRay detection rules, and Automated IOC classification can be used to **automate threat hunting without any additional filtering or human manipulation**.



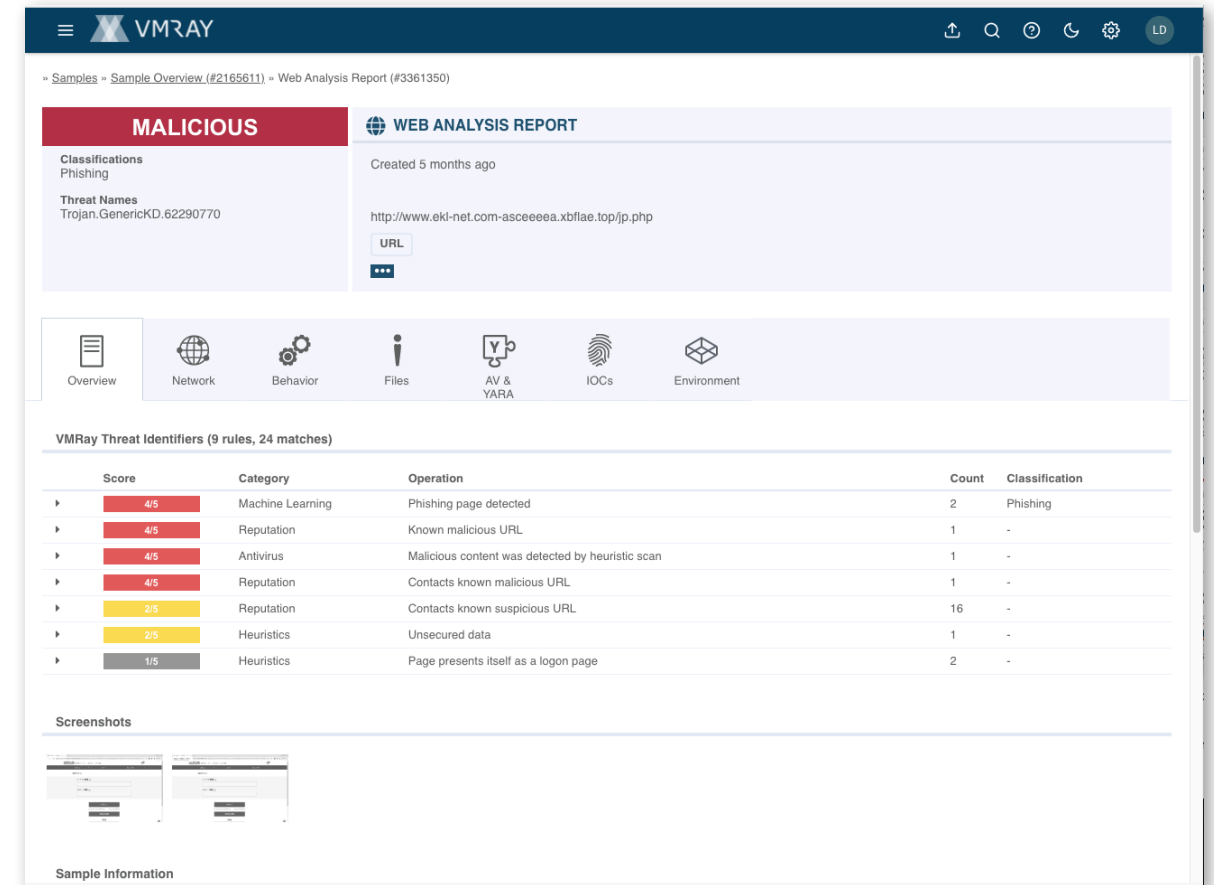
How User Reported Phishing Triage and Analysis Works:

1. **SOC Team enables Abuse Mailbox** then deploys the Outlook auto-submit plug-in to each Office365 end-user.
2. Trained on phishing attacks, an **end-user identifies a potentially malicious email** and **one-click auto-forwards it** to the company's preassigned Abuse Mailbox – example: <phishing@company123.com>.
3. **VMRay initially inspects the sender information** along with the originating IP and mail server to identify a forged email.



How User Reported Phishing Works

4. Email attachments and embedded URLs are then submitted to the reputation engine which contains a database of known malicious file hashes, known benign file hashes, and referenced URLs prior to starting deeper analysis. **If identified, previously known malicious files and web links are immediately flagged within seconds.**
5. The first stage after the reputation assessment is static analysis, which parses the suspicious phishing email or file attachment through a **multi-stage analysis process.**



The screenshot displays the VMRAY interface for a 'WEB ANALYSIS REPORT'. The report is classified as 'MALICIOUS' and shows a 'Threat Names' of 'Trojan.GenericKD.62290770'. The URL being analyzed is 'http://www.eki-net.com-asceeeea.xblflae.top/jp.php'. Below the report details, there is a navigation bar with icons for Overview, Network, Behavior, Files, AV & YARA, IOCs, and Environment. The main section shows 'VMRay Threat Identifiers (9 rules, 24 matches)' with a table of results.

Score	Category	Operation	Count	Classification
4/5	Machine Learning	Phishing page detected	2	Phishing
4/5	Reputation	Known malicious URL	1	-
4/5	Antivirus	Malicious content was detected by heuristic scan	1	-
4/5	Reputation	Contacts known malicious URL	1	-
2/5	Reputation	Contacts known suspicious URL	16	-
2/5	Heuristics	Unsecured data	1	-
1/5	Heuristics	Page presents itself as a logon page	2	-

Below the table, there are 'Screenshots' and 'Sample Information' sections.

How User Reported Phishing Works

6. If no matches are found in the reputational and static analysis stages, the URLs and any attached files are **detonated and analyzed to reveal any malicious behavior**.
7. For links that reach out to external sites, **VMRay follows all the links with multiple hops** and determines whether the sites are **malicious or not**.
8. **The end-user and SOC team are alerted** if the submission is found to be malicious.

MALICIOUS

Classifications: Downloader | Injector | Spyware | Exploit

Threat Names: C2/Generic-A | Mal/HTMLGen-A | XLoader

30 Hosts Requests Severity

Host	Requests	Severity
www.zservers.xyz	80	80
www.goehgy.store	80	80
www.pädotrychler.ch	80	80
agenciajcturismo.com	80	80
www.twin68s.online	80	80

VMRay Threat Identifiers (33 rules, 123 matches)

Score	Category	Operation	Count	Classification
5/5	System Modification	Modifies operating system directory	5	-
5/5	Input Capture	Captures clipboard data	1	Spyware
5/5	YARA	Malicious content matched by YARA rules	3	Spyware
5/5	Data Collection	Combination of other detections shows multiple input capture behaviors	1	Spyware
4/5	Anti Analysis	Tries to detect kernel debugger	1	-
4/5	Obfuscation	Reads from memory of another process	3	-
4/5	Hide Tracks	Deletes file after execution	1	-
4/5	Exploit	Exploits a vulnerability in MS Office	1	Exploit
4/5	Network Connection	Performs DNS request	15	-
4/5	Network Connection	Connects to remote host	15	-

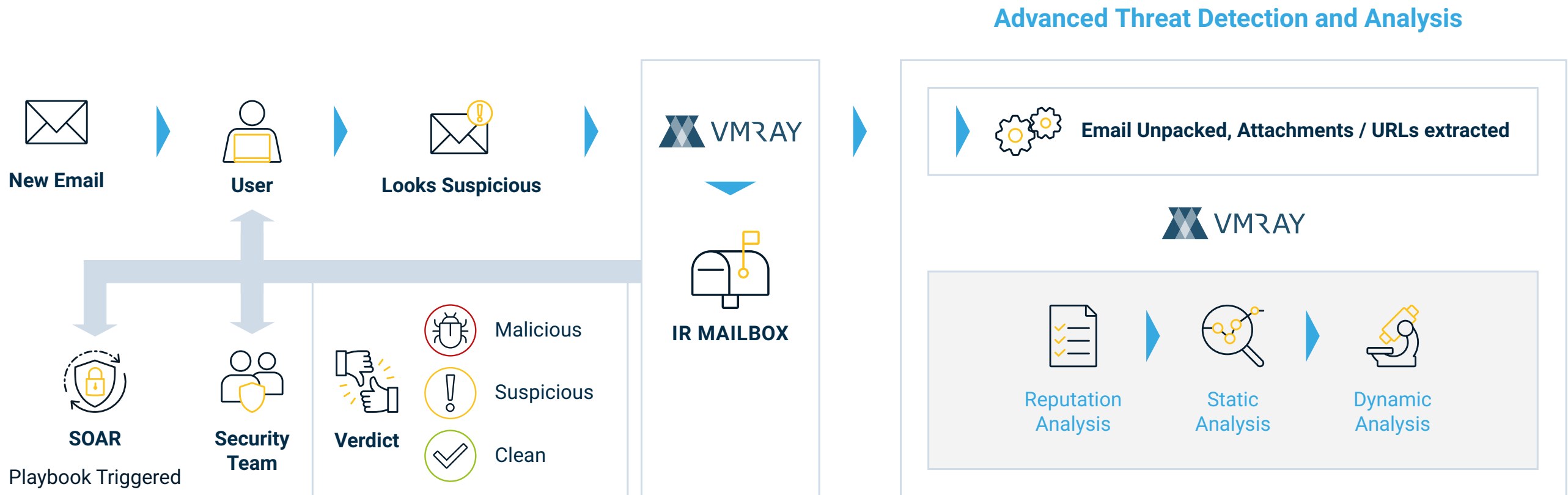
cloudways-static-content.s3.us-...

gmpg.org

Process flow diagram showing interactions between #11 ngenlask.exe, #12 addinprocess32.exe, #13 according yes.exe, #14 systay.exe, and #15 explorer.exe.

```
graph LR; #11[ngenlask.exe] -- "Modify Control Flow" --> #12[addinprocess32.exe]; #11 -- "Modify Memory" --> #12; #11 -- "Child Process" --> #12; #12 -- "Modify Control Flow" --> #13[according yes.exe]; #12 -- "Modify Memory" --> #13; #12 -- "Injection" --> #13; #13 -- "Child Process" --> #14[systay.exe]; #14 -- "Modify Memory" --> #15[explorer.exe]; #14 -- "Modify Control Flow" --> #15; #14 -- "Injection" --> #15;
```


Mitigate Email Threats at Speed



Deep Content Extraction

Fully extracting all the embedded content from samples, no matter how deep they are hidden. After extraction these objects are sent for further analysis. This includes **extracting embedded objects and links** from documents, links and attachments from emails, archive unpacking with no depth limit, as well as **decrypting password protected samples**.



Computer Vision

An important part of detection & analysis is the ability to **extract text from images** using Optical Character Recognition (OCR) to **detect social engineering techniques** used in phishing campaigns.



Smart Link Detonation

Attribute-based rules that **determine if links** embedded in emails and documents **should be detonated** for example, domain age, reputation score, abnormal URL string.



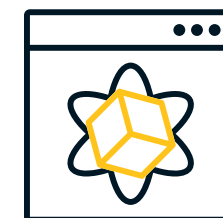
Password-Protected File Analysis

Protection against malicious password-protected attachments by **searching for passwords in the email body and subject**.



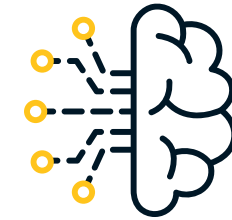
Adaptive Browser Simulation

Certain phishing attacks delivered via web pages may only be triggered if the user clicks on a button for example, a download button on file sharing site. This technology **detects and simulates the user interaction to automatically trigger payload delivery**.



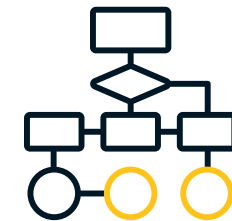
Machine Learning

Fed by high quality input data derived from the VMRay analysis, machine learning is used to **identify hard to detect phishing and credential harvesting attacks**.



Automated User Interaction

Simulation of user behavior to **spooft evasive malware into detonation** so analysis can continue. This includes mouse movements and clicks, as well as clicking on dialog boxes and providing expected responses.



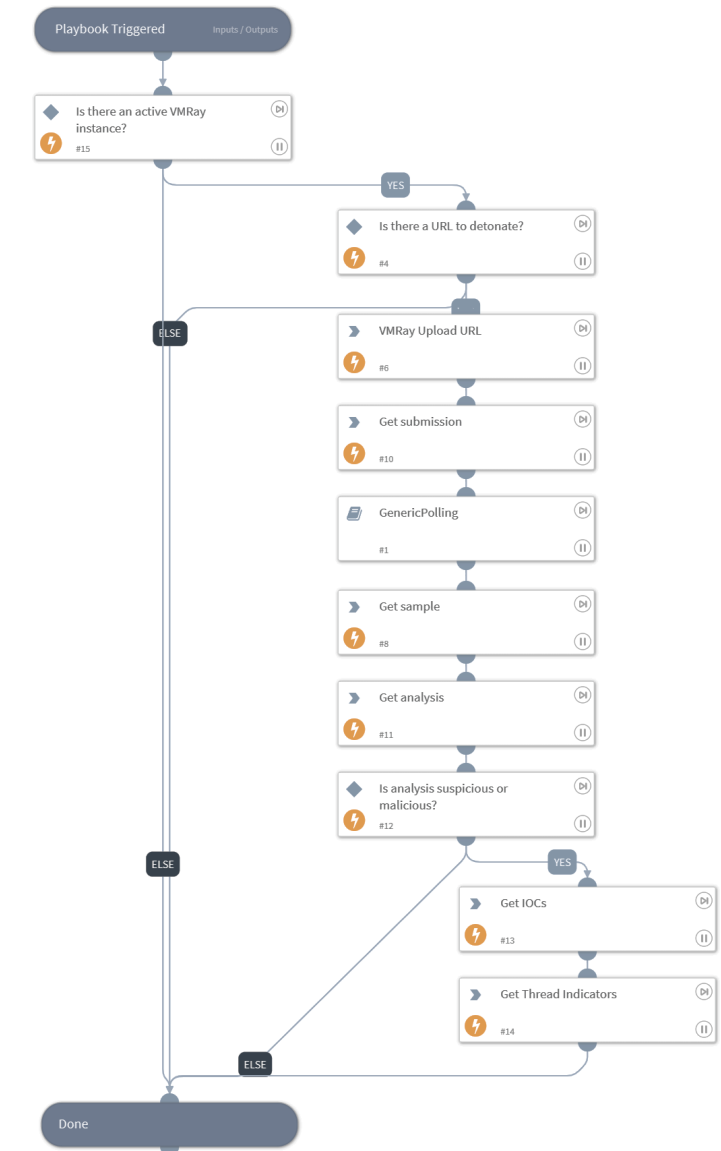
Live Interaction

Allows malware Analysts to **manually interact with the sample** during Dynamic File Analysis and Dynamic Web Analysis



The automation of phishing emails can be achieved using a SOAR solution with predefined playbooks to route emails and file attachments to VMRay for analysis.

1. The organization's perimeter-based phishing/SPAM solution **identifies elements** on an inbound email and **flags them as "suspicious"**.
2. The perimeter phishing/SPAM solution **creates an alert** and the **email is forwarded to the SOAR**. The **SOAR routes to email to VMRay** based on the playbook for further analysis.
3. **The file and URLs are detonated and analyzed** and the results of malicious or benign returned to the SOAR, in addition to notifications sent to the SOC and end-user.



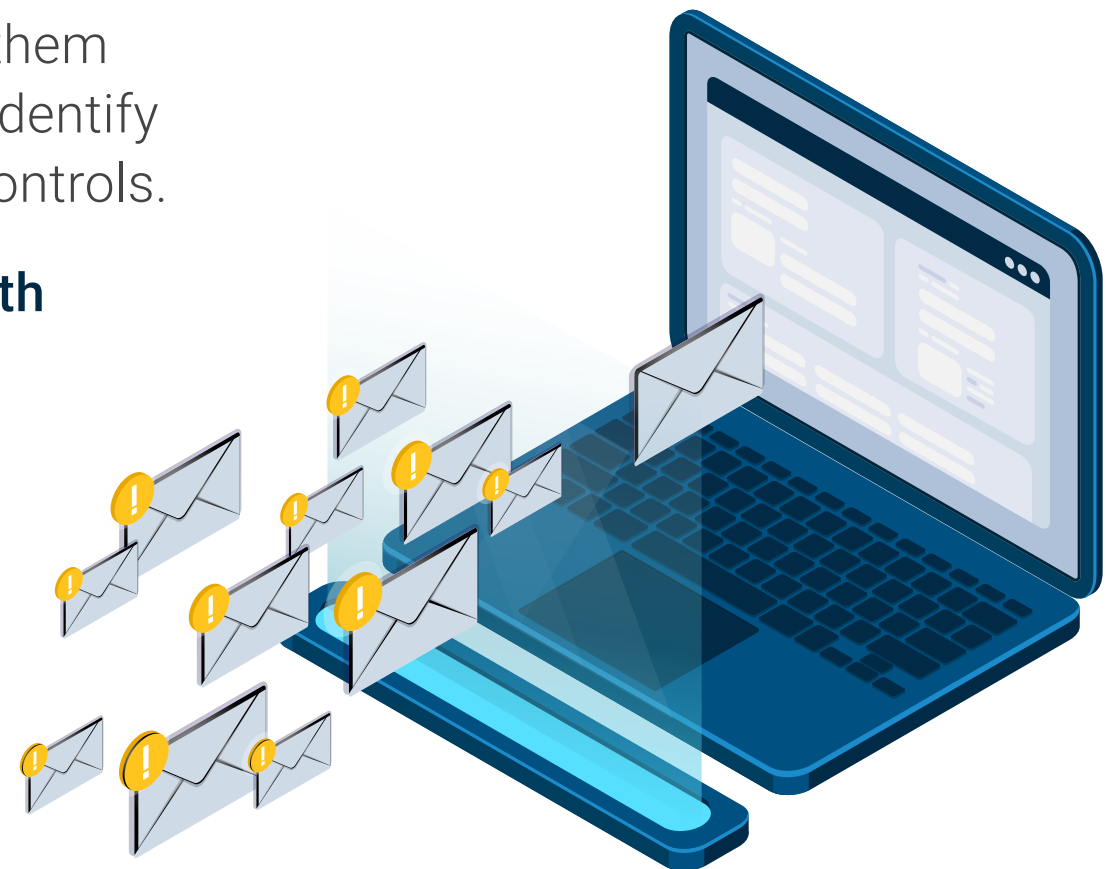
User Reported Phishing

Manual processing and triage of potentially malicious messages for further analysis **is time and resource intensive**.

Educating end-users on phishing attacks and how to detect them **helps the SOC team and adds another layer of detection** to identify malicious emails that have bypassed their primary security controls.

VMRay enables SOC teams to create a **dedicated mailbox with automated sandbox analysis** of user submitted emails and attachments. Triage and analysis can also be **automated via a SOAR playbook**.

The VMRay automated analysis comprises of **27 different technologies** and provides a **definitive third-party verdict** of malicious or benign, along with IOCs that help to mitigate the threat.



Automating Malware Triage and Analysis

Company Overview

A **cloud** and **on-premise** advanced threat detection and analysis platform.

VMRay enables enterprise and service provider SOC teams to analyze and extract the IOCs of **previously unknown, highly evasive malware** to quickly mitigate current and future threats.

With VMRay's ability to **scale and automate** Tier 1 / 2 triage in **high volume alert** environments, SOC teams can **improve economy of service** to meet SLAs with **fewer skilled malware analysts**.

VMRay Solutions



DeepResponse

Manual Malware Triage and Phishing Analysis



FinalVerdict

Automated Threat Detection and Analysis

















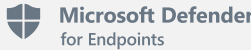













TotalInsight

Manual & Automated Threat Intelligence Extraction

Why do SOC Teams Like Working With Us?

Our integrations help augment the existing tech stack

SIEM	SOAR			
    	  	  	 	 
EDR / XDR	THREAT INTELLIGENCE			
     	  	 	 	



For more information, please visit vmray.com

Contact Us

Email: sales@vmray.com
Phone: +1 888 958-5801

VMRay GmbH

Suttner-Nobel-Allee 7
44803 Bochum ♦ Germany

VMRay Inc.

75 State Street, Ste 100
Boston, MA 02109 ♦ USA

