Homeland Security

# Analysis of Cyber-Attacks on US Assets

# America's #1 Cyber Threat: Phishing

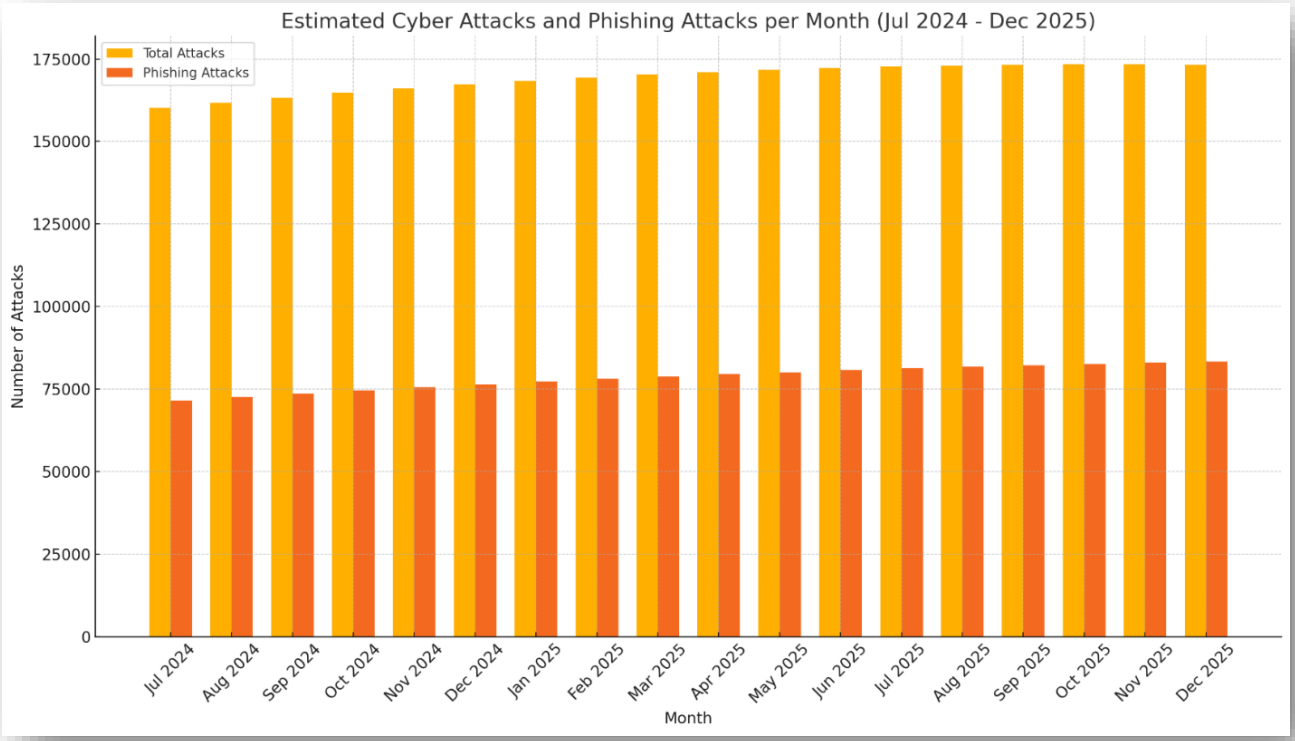
## (Spear Phishing, Whaling, Clone/Voice/SMS phishing)

By Casey Miles

**FOCUS PAPER:** Cyber-Attack trends over the next 18 months, their financial impact, and how to defend against them.

**ANSWER:** Phishing attacks and the resulting costs of successful Ransomware campaigns are costing America the most money.

**Reasoning:** Based on averaging statistical linear regressions and polynomial fitting to historical data, the chart below shows the number of cyber-attacks that are predicted in the US over the next 18 months:




This chart helps visualize that nearly half of all cyber-attacks on US assets are phishing attacks (definitions of all terms are at the end of this report). These phishing attacks typically contain malicious attachments or links to malicious websites that are focused on compromising, breaching, or holding ransom sensitive information. Reducing phishing will reduce many other and more serious cyber-threats.

Below are solutions that have the highest potential for reducing/eliminating this phishing epidemic. The DoD uses the Microsoft 360's suite of products widely across many departments. With that in mind, I've included a point on how these solutions integrate with that software suite.

**Lockheed Martin - Palantir Foundry**

- **Phishing Reduction:** Aggregates and analyzes data from multiple sources to identify phishing patterns. Automates blocking phishing emails based on detected patterns.
- **Data Collection:** Collects email metadata, content, and network traffic data. Uses APIs and network taps to gather information in real-time.
- **Integration with Microsoft 365**: Uses APIs to connect with Microsoft 365 email services, monitoring email traffic for phishing attempts and integrating with Microsoft Defender for Office 365 for enhanced threat detection and response.

**Northrop Grumman - ShieldAI**

- **Phishing Reduction:** Uses machine learning to recognize and block phishing emails. Continuously updates its database with new phishing tactics to stay ahead.
- **Data Collection:** Gathers email headers, body content, and user interaction data. Utilizes email gateways and machine learning sensors.
- **Integration with Microsoft 365**: Integrates with Microsoft 365 via email gateways and API connections, enabling seamless monitoring and protection of email communications. Works alongside Microsoft Defender to provide comprehensive phishing protection.

**Raytheon Technologies - SureView Insider Threat**

- **Phishing Reduction:** Monitors employee email behaviors to identify suspicious activity. Automatically flags and quarantines potential phishing emails.
- **Data Collection:** Collects user activity logs, email content, and access patterns. Deploys agents on endpoints and integrates with email servers.
- **Integration with Microsoft 365**: Deploys agents that monitor Microsoft 365 email usage patterns and integrates with the Microsoft 365 security dashboard to flag and isolate suspicious emails.

**BAE Systems - CyberReveal**

- **Phishing Reduction:** Analyzes email content and metadata to detect phishing attempts. Automates response by blocking and reporting phishing emails.
- **Data Collection:** Gathers email metadata, communication patterns, and attachment scans. Uses email server integration and content filters.
- **Integration with Microsoft 365**: Connects with Microsoft 365 email services to scan and analyze email traffic in real-time. Uses API integrations to block and report phishing emails within the Microsoft 365 environment.

**Science Applications International Corporation (SAIC) - CognitiQ**

- **Phishing Reduction:** Uses AI to analyze email traffic and detect phishing. Blocks suspicious emails and informs users to prevent phishing attacks.
- **Data Collection:** Collects network traffic, email content, and user behavior data. Employs network sensors and email proxies.
- **Integration with Microsoft 365**: Integrates with Microsoft 365's email services through APIs, enabling real-time analysis and blocking of phishing emails. Enhances the capabilities of Microsoft Defender for Office 365.

Implementing one or a few of the above solutions, at the right locations in the network, has the greatest potential to lower the overall cost of cyber-attacks and reduce the number of successful attacks.

The remainder of this paper further defines what the cyber attacks are, the financial impact of cyber-crime, and additional solutions to further mitigate the risk of loss.

## Additional information and analysis:

While phishing attacks account for the vast majority of cyber-attacks on US assets, they are far from the most expensive. However, they do “open the door” for other kinds of cyber-attacks that carry a much greater payload. Here are the numbers behind what each kind of attack is costing organizations and the average success rates of these attacks.

Average Cost **Per Attack** by Type:

**Ransomware** Attacks: $1,540,000 USD per successful attack.

- Based on data from Sophos and Rapid7, the average cost for a ransomware attack recovery in 2023 was approximately $1.54 million, which includes ransom payments and recovery costs.
- Number of Successful Attacks: 59.7% of ransomware attacks result in a ransom being paid. This means approximately 59.7% of the total ransomware attacks will incur this cost.
- Sources: Varonis, Sophos

Distributed Denial of Service (**DDoS**) Attacks: $120,000 USD

- According to Comparitech, DDoS attacks can vary widely in cost, but the average is around $120,000, including mitigation and downtime costs.
- Number of Successful Attacks: Approximately 15-20% of DDoS attacks are successful in causing significant disruption.
- Sources: Comparitech, Varonis

**Data Breaches**: $4,450,000 USD

- IBM's Cost of a Data Breach Report 2023 states that the average cost of a data breach was $4.45 million globally.
- Number of Successful Attacks: About 10-15% of data breach attempts result in significant data loss or exposure.

- Sources: IBM, Varonis
- Data breaches are more of a focus for classified and sensitive information. Data breaches are rarely successful, however when they are, they can cause significant damage to US Govt. assets, missions, and critical infrastructure and should be considered one of the central focuses of our nation's cyber-defense.

**Malware** Attacks: $250,000 USD

- The average cost for malware attack remediation, according to Rapid7, is around $250,000, considering the impact on systems and recovery efforts.
- Number of Successful Attacks: Roughly 30% of malware attacks lead to substantial damage or data loss.
- Sources: Rapid7, Varonis

**Man-in-the-Middle** (MitM) Attacks: $100,000 USD

- MitM attacks typically cost around $100,000 due to the complexity of detecting and mitigating these threats, including legal and remediation costs.
- Number of Successful Attacks: Around 10-15% of MitM attacks successfully intercept sensitive information.
- Sources: Sophos

**SQL Injection** Attacks: $200,000 USD

- SQL injection attacks can cause significant damage, averaging around $200,000 in recovery costs, according to cybersecurity industry reports.
- Number of Successful Attacks: Approximately 10-15% of SQL injection attempts result in unauthorized data access.
- Sources: Varonis

**Zero-Day Exploits**: $2,000,000 USD

- These attacks are highly costly, often averaging $2 million due to the need for specialized recovery efforts and the impact on critical systems.
- Number of Successful Attacks: About 5% of zero-day exploits are successful, given their complexity and targeted nature.
- Sources: Sophos

**Credential Stuffing**: $200,000 USD

- Credential stuffing attacks average around $200,000, including costs related to system breaches and user data recovery.
- Number of Successful Attacks: Around 8-10% of credential stuffing attempts lead to unauthorized account access.
- Sources: Varonis

Advanced Persistent Threats (**APTs**): $1,000,000 USD

- APTs are sophisticated and prolonged attacks, costing on average $1 million, including extensive recovery and investigation efforts.
- Number of Successful Attacks: Approximately 5% of APTs successfully infiltrate and persist within networks.
- Sources: Sophos

**Social Engineering** Attacks: $150,000 USD

- The cost of social engineering attacks, which often include phishing, averages $150,000 due to their impact on employee systems and data integrity.
- Number of Successful Attacks: Around 30% of social engineering attempts result in a successful breach.
- Sources: Varonis

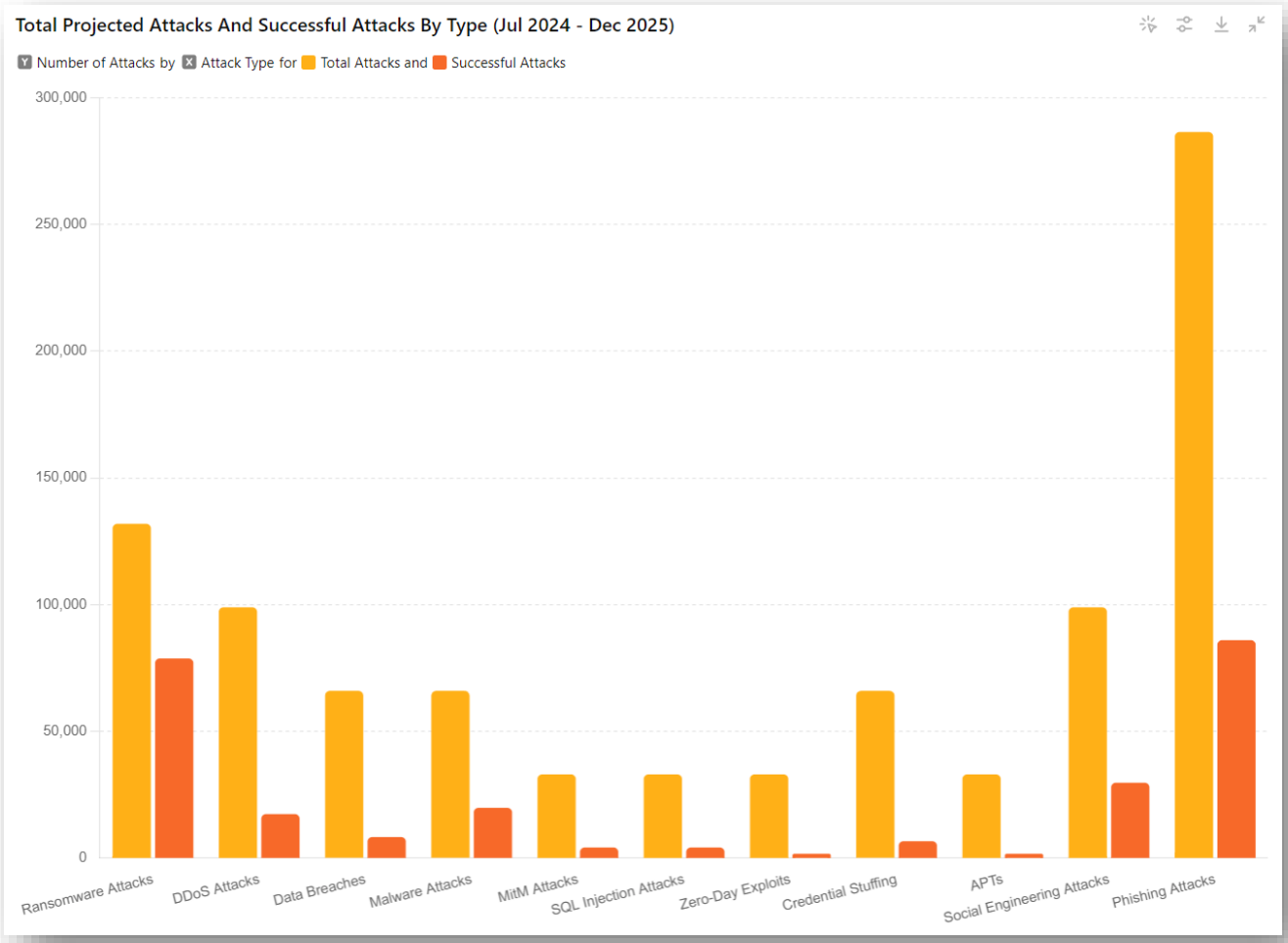
**Phishing** Attacks: $20,000 USD

- Phishing attacks are generally less costly per incident, averaging around $20,000, primarily due to their frequency and simpler mitigation measures.
- Number of Successful Attacks: Phishing attacks have a success rate of approximately 30%, leading to compromised credentials or financial loss.
- Sources: Sophos

Sources for the above information:


1. **Varonis** Ransomware Statistics: https://www.varonis.com/blog/ransomware-statistics
2. **Sophos** State of Ransomware 2023: https://assets.sophos.com/X24WTUEQ/at/sophos-state-of-ransomware-2023-wp.pdf
3. **Comparitech** Ransomware Statistics: https://www.comparitech.com/blog/information-security/ransomware-statistics/
4. **IBM** Cost of a Data Breach Report 2023: https://www.ibm.com/reports/data-breach
5. **Rapid7** 2023 Ransomware Stats: https://www.rapid7.com/blog/post/2024/01/12/2023-ransomware-stats-a-look-back-to-plan-ahead/
6. **Backblaze** The True Cost of Ransomware: https://www.backblaze.com/blog/the-true-cost-of-ransomware/

Considering the total number of attacks from the first chart and the statistics of successful attacks presented in the above list, this is a look at how many attacks, of each kind, are projected to happen in the next 18 months. The first bar is the total number of attacks of each kind, the second bar is the anticipated number of successful attacks of each kind.



Historically, cyber-crime has had a growing financial impact. In 2021, cyber-crime tallied $6.9 billion in losses as reported to the FBI Internet Crime Complaint Center (IC3). In 2022, that figure jumped by 49.3% to $10.3 billion! While 2023 isn't fully compiled yet, expectations are around $15.4 billion for 2023 and $23 billion for 2024.

Breakdown of the largest contributors to losses due to **cyber-crime in 2022**:

Ransomware Attacks:

- Total Incidents: 2,385
- Total Adjusted Losses: $34.3 million
- Source: FBI IC3 2022 Report

Phishing and Related Scams:

- Total Incidents: 300,000 (approximately)
- Total Losses: Data not specific but forms a significant portion of the overall $10.3 billion.
- Source: FBI IC3 2022 Report

Investment Fraud:

- Total Losses: $3.31 billion
- Source: SecurityWeek

Business Email Compromise (BEC):

- Total Incidents: Over 21,000
- Total Losses: $2.7 billion
- Source: SecurityWeek

By combining the anticipated number of successful attacks and the historical average cost of each kind of attack, we can estimate the following costs from July of 2024 to December of 2025 (**18 month prediction**):

Reconciled Data for All Attack Types:

Ransomware Attacks

- Total Attacks: 30,667
- Total Successful Attacks: 18,315 (59.7%)
- Successful Attacks Resulting in Payment: 5,312 (29%)
- Average Cost per Attack: $150,000
- Total Cost: $4,597,800,000

DDoS Attacks

- Total Attacks: 69,000
- Total Successful Attacks: 12,075 (17.5%)
- Average Cost per Attack: $50,000

- Total Cost: $3,450,000,000

Data Breaches

- Total Attacks: 767
- Total Successful Attacks: 96 (12.5%)
- Average Cost per Attack: $3,000,000
- Total Cost: $2,300,000,000

Malware Attacks

- Total Attacks: 92,000
- Total Successful Attacks: 27,600 (30.0%)
- Average Cost per Attack: $100,000
- Total Cost: $2,300,000,000

Man-in-the-Middle (MitM) Attacks

- Total Attacks: 46,000
- Total Successful Attacks: 5,750 (12.5%)
- Average Cost per Attack: $50,000
- Total Cost: $287,500,000

SQL Injection Attacks

- Total Attacks: 46,000
- Total Successful Attacks: 5,750 (12.5%)
- Average Cost per Attack: $100,000
- Total Cost: $575,000,000

Zero-Day Exploits

- Total Attacks: 15,333
- Total Successful Attacks: 767 (5.0%)
- Average Cost per Attack: $1,000,000
- Total Cost: $767,000,000

Credential Stuffing

- Total Attacks: 92,000
- Total Successful Attacks: 9,200 (10.0%)
- Average Cost per Attack: $50,000
- Total Cost: $460,000,000

Advanced Persistent Threats (APTs)

- Total Attacks: 15,333
- Total Successful Attacks: 767 (5.0%)
- Average Cost per Attack: $500,000

- Total Cost: $383,500,000

Social Engineering Attacks

- Total Attacks: 69,000
- Total Successful Attacks: 20,700 (30.0%)
- Average Cost per Attack: $75,000
- Total Cost: $1,552,500,000

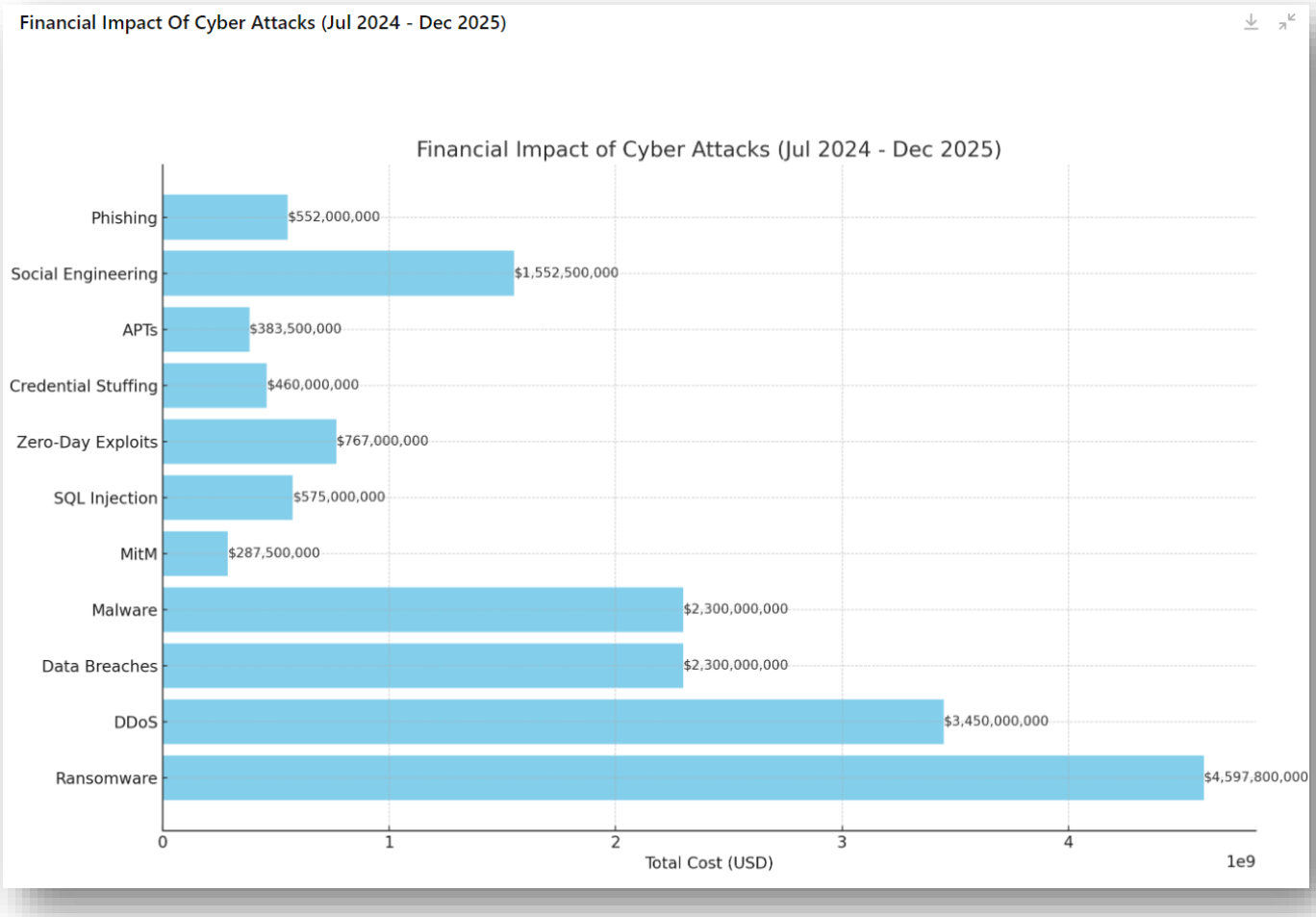
Phishing Attacks

- Total Attacks: 184,000
- Total Successful Attacks: 55,200 (30.0%)
- Average Cost per Attack: $10,000
- Total Cost: $552,000,000

**Summary of Adjusted Projections**

Total Projected Cost: **$23,615,300,000** (spread over 18 months, adjusted to historical trends and median costs)

The above costs are visually summarized in this chart:



What stands out is that ransomware is costing America a lot of money. However, the leading **Ransomware attacks are perpetrated through phishing emails**. From the first chart in this report, that shows phishing emails as over 40% of all cyber-attacks combined, it can be understood that the most costly kind of attacks are perpetrated through the most frequent kind of attacks. To put plainly, eliminating/reducing phishing attacks will result in reducing ransomware attacks. This falls into the adage of "An ounce of protection is worth 4.5 billion dollars of cure".

Here are the leading ransomware attacks affecting US assets today that are typically delivered through phishing emails:

**Ryuk**

- Description: A sophisticated ransomware known for targeting large enterprises and government organizations.
- **Infection Method:** Often delivered through phishing emails with malicious attachments, or via secondary infections through other malware like Emotet and TrickBot.
- Impact: Encrypts critical files and demands high ransom payments in Bitcoin.

**Sodinokibi (REvil)**

- Description: A ransomware-as-a-service (RaaS) operation that allows affiliates to use its platform for a share of the profits.
- **Infection Method:** Exploits vulnerabilities in remote desktop protocols (RDP), software vulnerabilities, and phishing campaigns.
- Impact: Encrypts files and threatens to release stolen data if the ransom is not paid.

**Maze**

- Description: Known for its "double extortion" tactic, where it encrypts data and threatens to release it publicly.
- **Infection Method:** Phishing emails, exploit kits, and compromised websites.
- Impact: Encrypts files and exfiltrates data, demanding ransom payments to avoid data leaks.

**Dharma (CrySIS)**

- Description: A persistent ransomware variant that continues to evolve.
- **Infection Method:** RDP brute force attacks and phishing emails.
- Impact: Encrypts files and demands payment in Bitcoin for decryption keys.

**LockerGoga**

- Description: Often targets industrial and manufacturing firms.
- **Infection Method**: Spear-phishing emails and compromised software updates.
- Impact: Encrypts files and disrupts operations, leading to significant downtime and financial loss.

**WannaCry**

- Description: Gained notoriety for its rapid spread and significant impact on organizations worldwide in 2017.
- Infection Method: Exploits the EternalBlue vulnerability in Windows SMB protocol.
- Impact: Encrypts files and demands ransom payments in Bitcoin, causing widespread disruption.

**Conti**

- Description: Known for its speed and efficiency in encrypting files.
- **Infection Method:** Phishing emails, malicious attachments, and exploiting vulnerabilities in RDP.
- Impact: Encrypts data and uses double extortion tactics, demanding ransom to decrypt data and prevent data leaks.

While the software solutions previously listed in this report can help prevent phishing attacks, they won't help when you're in the middle of the resulting Ransomware attack. Below are the leading solutions to prevent ransomware attacks and break assets out of ransomware attacks when the phishing campaign found a phish and set the hook. In addition to including a point on integrating these solutions with Microsoft 360's suite of products as before, I've added how they use Ai/ML to perform their tasks.

**Northrop Grumman - ShieldAI**

- **Ransomware Prevention**: AI-driven threat detection, automated response, and continuous monitoring to identify and mitigate ransomware attacks.
- **Integration**: Collects data from network traffic, endpoint sensors, and existing security infrastructure. Integrates with SIEM (Security Information and Event Management) systems and endpoint protection platforms.
- **AI Use**: Utilizes machine learning models to detect anomalies and patterns indicative of ransomware and automates responses to neutralize threats.
- **Integration with Microsoft 365**: Integrates with Microsoft 365 security tools and Microsoft Defender for Endpoint. Provides continuous monitoring and automated response to potential ransomware threats targeting Microsoft 365 environments.

**Lockheed Martin - Cyber Kill Chain**

- **Ransomware Prevention**: Advanced data integration and analytics, real-time threat detection, and automated blocking of ransomware.
- **Integration**: Aggregates data from various sources including network logs, endpoint data, and threat intelligence feeds. Uses APIs to connect with existing security tools and platforms.
- **AI Use**: Employs AI for predictive analytics and real-time threat identification, enhancing the ability to prevent and respond to ransomware attacks.

- **Integration with Microsoft 365**: Utilizes APIs to aggregate data from Microsoft 365 services, including OneDrive, SharePoint, and Teams. Integrates with Microsoft Defender to enhance ransomware detection and response.

**Raytheon Technologies - SureView Threat Protection**

- **Ransomware Prevention**: Real-time threat monitoring, user behavior analytics, and automated incident response to prevent ransomware propagation.
- **Integration**: Monitors user activity and network traffic. Deploys agents on endpoints and integrates with email security solutions and firewalls.
- **AI Use**: Uses AI to analyze user behavior and network anomalies, triggering automated responses to potential ransomware threats.
- **Integration with Microsoft 365**: Monitors Microsoft 365 user activity and integrates with Microsoft Defender for Endpoint. Deploys agents on Microsoft 365 endpoints to detect and respond to ransomware threats.

**BAE Systems - CyberReveal**

- **Ransomware Prevention**: AI-driven threat detection, comprehensive situational awareness, and automated response to ransomware incidents.
- **Integration**: Collects and analyzes data from network devices, endpoints, and cloud environments. Integrates with threat intelligence platforms and security orchestration tools.
- **AI Use**: Leverages AI for deep analysis of network and endpoint data to detect sophisticated ransomware attacks and automate defensive actions.
- **Integration with Microsoft 365**: Collects data from Microsoft 365 services, including email, OneDrive, and SharePoint. Integrates with Microsoft 365 security tools to provide enhanced threat detection and automated responses.

**General Dynamics - TITAN**

- **Ransomware Prevention**: Advanced threat detection, machine learning algorithms, and real-time monitoring to prevent ransomware.
- **Integration**: Gathers data from network sensors, endpoint detection and response (EDR) systems, and security analytics platforms. Uses APIs to integrate with existing cybersecurity infrastructure.
- **AI Use**: Utilizes machine learning algorithms to detect and respond to ransomware attacks in real-time, improving the speed and accuracy of threat mitigation.
- **Integration with Microsoft 365**: Gathers data from Microsoft 365 environments, using APIs to integrate with Microsoft Defender for Endpoint and other Microsoft 365 security tools. Provides real-time monitoring and automated threat mitigation within the Microsoft 365 ecosystem.

## Conclusion

A combination of the anti-phishing solutions and the ransomware solutions, integrated to Microsoft 360's suite of applications, is the recommended path to reduce total number of cyber-attacks and the financial impact on our government infrastructure. Implementing these functions at the highest levels of the network architecture, ie. border routers (logs, interface data) and eMail relays (scanning attachments and send-from locations), in addition to implementing them at the directorate level, will ensure multiple layers of security, enable our talented sysadmins to discover new methods of threat detection & prevention, and provide for an evolving ecosystem of IT professionals in the cyber warfare space to have the tools they need and sandbox capabilities to adjust to the threats of tomorrow. It will also have the potential to save America $23B in annual losses due to cyber-crime.

Definitions: Types of cyber-attacks

Ransomware Attacks

- Definition: Malware that encrypts data and demands payment for the decryption key.
- Targets: Government agencies, military installations, and defense contractors. These attacks can disrupt operations and compromise sensitive information.

Distributed Denial of Service (DDoS) Attacks

- Definition: Overloading a network, service, or website with traffic to render it unusable.
- Targets: Government websites, military communication networks, and public service systems. DDoS attacks can prevent access to critical services and information.

Data Breaches

- Definition: Unauthorized access and retrieval of sensitive data.
- Targets: Government databases, defense contractor systems, and DHS repositories. Data breaches can lead to the exposure of classified information and personal data of government employees.

Malware Attacks

- Definition: Software designed to disrupt, damage, or gain unauthorized access to computer systems.
- Targets: Defense networks, government infrastructure, and DHS systems. Malware can sabotage operations, steal data, and create backdoors for further exploits.

Man-in-the-Middle (MitM) Attacks

- Definition: Eavesdropping on communication between two parties to steal or alter data.
- Targets: Secure government communications, military transmissions, and DHS communications. MitM attacks can compromise the integrity and confidentiality of sensitive communications.

SQL Injection Attacks

- Definition: Inserting malicious SQL code into a query to manipulate a database.
- Targets: Government websites, defense contractor databases, and DHS applications. These attacks can exfiltrate data or alter critical database information.

Zero-Day Exploits

- Definition: Exploiting previously unknown vulnerabilities in software or hardware.
- Targets: Military systems, government software, and DHS tools. Zero-day exploits can be used to launch highly targeted and damaging attacks before patches are available.

Credential Stuffing

- Definition: Using stolen credentials to gain unauthorized access to user accounts.
- Targets: Government portals, military personnel accounts, and DHS employee systems. Credential stuffing can lead to unauthorized access to confidential systems and data.

Advanced Persistent Threats (APTs)

- Definition: Prolonged and targeted cyberattacks aimed at stealing data or conducting surveillance.
- Targets: National defense networks, critical infrastructure, and high-value government entities. APTs can result in long-term espionage and data exfiltration.

Social Engineering Attacks

- Definition: Manipulating individuals into divulging confidential information.
- Targets: Government employees, military personnel, and DHS staff. Social engineering can bypass technical defenses by exploiting human vulnerabilities.

Phishing Attacks

- Definition: Fraudulent attempts to obtain sensitive information by disguising itself as a trustworthy entity.
- Targets: Government email users, military personnel, and DHS employees. Phishing attacks can lead to credential theft, data breaches, and malware infections.

# Phishing attacks further defined (referenced in the title)

**Email Phishing**

- Description: This is the most prevalent form of phishing, where attackers send fraudulent emails that appear to come from legitimate sources such as banks, social media sites, or other trusted entities. These emails often contain links to fake websites designed to steal personal information or credentials.
- Example: An email that appears to be from a bank asking the recipient to verify their account information by clicking a link.

**Spear Phishing**

- Description: Spear phishing is a targeted form of phishing where the attacker tailors their emails to a specific individual or organization. This type of attack is more personalized and often uses information gathered from social media or other sources to make the email appear more legitimate.
- Example: An email addressed directly to an employee of a company, appearing to come from their CEO, requesting sensitive information or urgent action.

**Whaling**

- Description: Whaling is a type of spear phishing that targets high-profile individuals such as executives, CEOs, or other senior officials within an organization. The emails are crafted to appear as legitimate business communications.
- Example: An email that looks like a legal subpoena or an urgent business request directed to the company's CEO.

**Clone Phishing**

- Description: In clone phishing, the attacker creates a near-identical copy of a legitimate email that the victim has previously received. The cloned email will often contain a malicious link or attachment.
- Example: A seemingly identical email to a previous one received from a trusted source, but with a different link that leads to a phishing site.

**Vishing (Voice Phishing)**

- Description: Vishing involves using phone calls to trick victims into providing personal information or performing actions that benefit the attacker. These calls often impersonate representatives from banks, government agencies, or tech support.
- Example: A phone call claiming to be from a bank's fraud department, asking the victim to verify their account information.

**Smishing (SMS Phishing)**

- Description: Smishing involves sending fraudulent text messages to victims, often containing links to phishing websites or phone numbers that lead to voice phishing.
- Example: A text message that appears to be from a delivery service, asking the recipient to click a link to track their package.

Sources:


- IBM Cost of a Data Breach Report - 2023 - https://www.ibm.com/reports/data-breach
- Rapid7 Ransomware Stats - 2023 - https://www.rapid7.com/blog/post/2024/01/12/2023-ransomware-stats-a-look-back-to-plan-ahead/
- Backblaze The True Cost of Ransomware - 2023 - https://www.backblaze.com/blog/the-true-cost-of-ransomware/
- Comparitech Ransomware Statistics - 2023 - https://www.comparitech.com/blog/information-security/ransomware-statistics/
- FBI IC3 Annual Report - 2022 - https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf
- SecurityWeek Cybercrime Losses Exceeded $10 Billion in 2022 - 2023 - https://www.securityweek.com/cybercrime-losses-exceeded-10-billion-2022-fbi
- World Economic Forum Global Risk Report - 2023 - https://www.weforum.org/reports/global-risk-report-2023
- Statista Cyber Crime Financial Loss in the US - 2023 - https://www.statista.com/statistics/627217/us-businesses-cyber-crime-financial-loss/
- Varonis Ransomware Statistics - 2023 - https://www.varonis.com/blog/ransomware-statistics
- Sophos State of Ransomware Report - 2023 - https://assets.sophos.com/X24WTUEQ/at/sophos-state-of-ransomware-2023-wp.pdf
- FBI Internet Crime Complaint Center (IC3) Report - 2022 - https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf
- Verizon Data Breach Investigations Report (DBIR) - 2023 - https://www.verizon.com/business/resources/reports/dbir/
- Anti-Phishing Working Group (APWG) Q1 Report - 2023 - https://apwg.org/trendsreports/
- Northrop Grumman - ShieldAI - 2023 - https://www.northropgrumman.com/cyber/shieldai/
- Lockheed Martin - Palantir Foundry - 2023 - https://www.palantir.com/platforms/foundry/
- Raytheon Technologies - SureView® Insider Threat - 2023 - https://www.raytheonintelligenceandspace.com/capabilities/cyber/sureview-insider-threat
- BAE Systems - CyberReveal - 2023 - https://www.baesystems.com/en/product/cyberreveal