THE WICKED BEASTS

OF THE

CYBERSECURITY WORLD

– AND HOW TO BEAT THEM

YOUR CYBERSECURITY MONSTER HUNTING GUIDE

The modern technology landscape is riddled with evils that go bump in the cloud. Pernicious cyber monsters lie in wait in the shadows, until BOOM! They attack, leaving you and your clients with a costly cleanup that can have lasting damage. But you can defend yourself against the nasties that haunt cybersecurity teams around the globe through education, preparing a strong security posture, and consistent action. Read on to learn all the spooky details.

BEWARE: CYBER THREAT CREATURES AHEAD!

RANSOMWAREWOLF

Do you hear that howling in the distance? That crying you hear is coming from organizations that have been hit by the Ransomwarewolf, a shifty threat that may disguise itself as a harmless .pdf or executable file via a social engineering attack that transforms into malware, which holds a victim's sensitive data or device hostage for payment.

RECENT VICTIMS

Ransomware is one of the more common cybersecurity threats out there, comprising 20% of all cyberattacks, according to the IBM® X-Force® Threat Intelligence Index. IBM also estimates this attack costs an average of $5.13 million – which doesn't even take ransom payments into account. Luckily, improvements in threat detection and prevention have been somewhat of a silver bullet, helping ransomware infections decline by 11.5% between 2022 and 2023.

HOW RANSOMWAREWOLF STRIKES

Ransomwarewolf is a sly beast and can take many shapes, including:

CRYPTO RANSOMWARE OR ENCRYPTORS:
This variant encrypts files and data within a system, rendering them inaccessible without a decryption key. Victims are then extorted for payment.

LOCKERS:
Lockers completely lock users out of their systems, preventing access to files and applications. A ransom demand is displayed, often with a countdown clock to increase urgency.

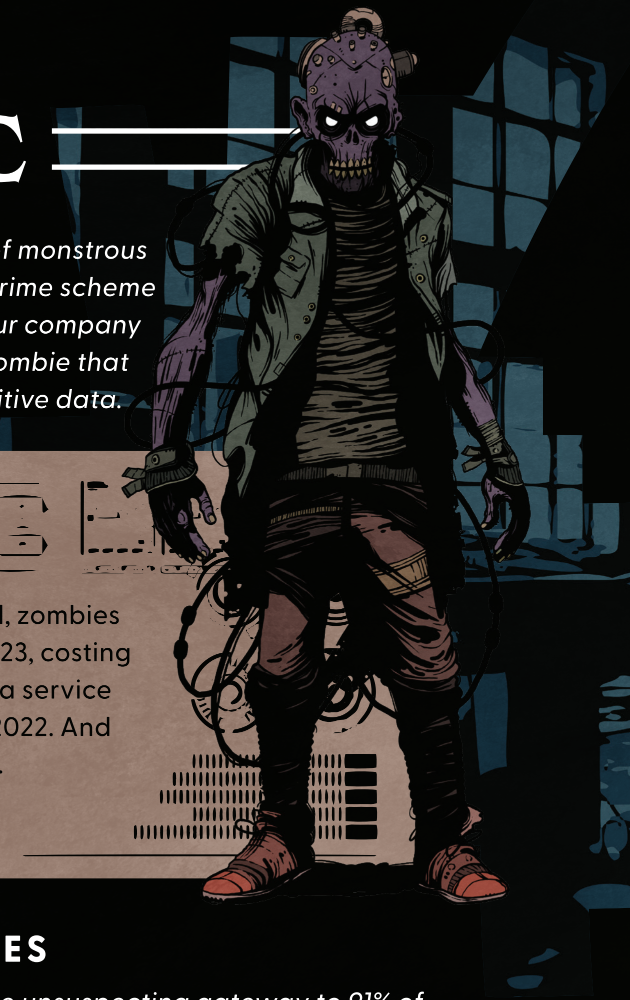
SCAREWARE:
Scareware masquerades as fake software, claiming to detect viruses or issues on a computer. It directs users to pay to resolve the problem, either by locking the computer or flooding the screen with alerts. Be afraid … be very afraid.

DOXWARE OR LEAKWARE:
Doxware copies sensitive personal or company information and threatens to expose it unless a ransom is paid. Variations include police-themed ransomware that warns of illegal online activity.

RAAS (RANSOMWARE AS A SERVICE):
RaaS refers to malware hosted anonymously by professional hackers who handle all aspects of the attack, from distribution to collecting payments, in exchange for a share of the loot.

ZOMBEC

Rising from the ground in recent years has been a cyber villain of monstrous proportions: ZomBEC, or business email compromise. This cybercrime scheme sees bad actors covering their malicious intention to devour your company intel or funds by posing as trusted figures via email. It's like a zombie that feasts on brains—only in this case, it's bank accounts and sensitive data.



RECENT VICTIMS

With the rise of remote work, BEC scams have multiplied like, well, zombies do. In fact, the FBI fielded more than 20,000 BEC complaints in 2023, costing U.S. orgs $4.57 billion in 2023. Microsoft noted that cybercrime as a service targeting business email saw a 38% increase between 2019 and 2022. And Kiteworks says BEC costs an average loss of $88,350 per incident.

HOW ZOMBEC STRIKES

ZomBEC feasts on email. While it may seem harmless, email is the unsuspecting gateway to 91% of cyberattacks. Let's delve into the shadowy realm of compromised emails and their deceptive guises:

DATA THEFT:
In this situation, scammers start by infiltrating the HR department and swiping company information like an unsuspecting employee's schedule or personal phone number. With this intel in hand, it's easier for them to unleash one or another BEC scam, making the whole charade seem eerily believable.

FALSE INVOICE SCHEME:
Disguised as a trusted vendor, the scammer sends a chillingly realistic fake invoice to your company. The account number might be just a single digit off, or they might insist you pay a different bank, claiming your current one is under audit.

CEO FRAUD:
These digital ghouls either spoof or hack into a CEO's email account, then send instructions to employees demanding they make purchases or wire money. The scammer might even direct an employee to buy gift cards and then send photos of the serial numbers, turning them into unwitting accomplices.

LAWYER IMPERSONATION:
In this scheme, attackers gain unauthorized access to an email account at a law firm, then email clients a phony invoice or a link to pay online. While the email address is legitimate, the bank account is a trap, leading victims into a financial nightmare.

ACCOUNT COMPROMISE:
Scammers deploy phishing or malware to take control of a finance employee's email account, such as an accounts receivable manager. With this access, they send the company's suppliers fake invoices, directing payments to a fraudulent bank account, draining funds into the abyss.

DOSULA

Your computer slows to a crawl. Typical functions take forever. With the lifeblood seemingly drained from your device, it can only be the work of one malicious monster. From out of the shadows, it's DOSula, or a denial of service (DOS) attack.

This attack can make a device or computer unusable by flooding it with requests until it can't process normal traffic. These requests suck up all the juice from a device or network until it can't respond or crashes. Then the baddies can do their worst, distracting users from their real target while they sink their teeth into other services within the network.

RECENT VICTIMS

DOS attacks take a sizable bite out of the cyberattack pie, representing 46% of total incidents in a 2022 analysis by Verizon. When it comes to distributed denial of services attacks (DDOS, covered below), Cloudflare says it mitigated more than 5.2 million HTTP DDOS attacks (which attempt to overwhelm HTTP servers) in 2023, a 20% decrease from 2022, but saw a rise in network-layer attacks, mitigating 8.7 million, an 85% increase from 2022.

HOW DOSULA STRIKES

DOSula can get its fangs through defenses in a number of ways:

DDOS ATTACK:
This happens when multiple machines swarm together to attack one target. These devilish attacks often use a botnet, or a group of hijacked internet-connected devices, to breach security vulnerabilities or device weaknesses and take control of numerous devices. The attacker can then use its army of newly created servants to unleash the DDoS on a target, making victims of both the infected devices and the end attack recipient.

SMURF ATTACK:
Far from what its cuddly name would suggest, this attack sends Internet Control Message Protocol broadcast packets to hosts with a phony source Internet Protocol (IP) address from the victim, causing the target to be flooded with responses.

SYN FLOOD:
As evil as it sounds, this happens when an attacker sends a request to connect to the target server but doesn't properly complete the connection, leaving the connected port in limbo, occupied and unavailable for new requests. The attacker continues to send requests, saturating all open ports so legitimate users can't connect.

PHISHENSTEIN

It's alive! Phishenstein, representing phishing scams, takes victims in its clutches by sending an email or text that seems to be from a well-known source, such as an internet service provider or a bank, and asks the recipient to provide personal identifying information, such as a credit card number, account number, passwords, or username. That's when Phishenstein attacks, opening new accounts, invading existing accounts, and causing all sorts of havoc for companies and individuals.

ATTACK TYPES

Phishenstein can take many guises, so it's always best to be on the lookout!

STANDARD EMAIL PHISHING:
Widely known, this attack aims to steal sensitive information through emails that appear to be from legitimate organizations. It's not targeted and can be conducted en masse.

MALWARE PHISHING:
Similar to email phishing, this attack tricks targets into clicking links or downloading attachments, installing malware on their devices. It's currently the most pervasive form of phishing.

SPEAR PHISHING:
This highly targeted attack is often aimed at business executives and public figures. Phishenstein can take advantage of his superhuman research capabilities to collect public information about these folk that can be used against them.

SMISHING:
HULK SMISH! In this attack, Phishenstein sends smartphone users malicious short links disguised as account notices or prize notifications, for example – only instead of winning a prize, they get SMISHED.

VISHING (VOICE PHISHING):
Malicious callers pretend to be tech support, government agencies, or other organizations to extract personal info like banking details.

PHARMING (DNS POISONING):
This venomous attack reroutes legitimate web traffic to spoofed pages without the user's knowledge, often stealing valuable data.

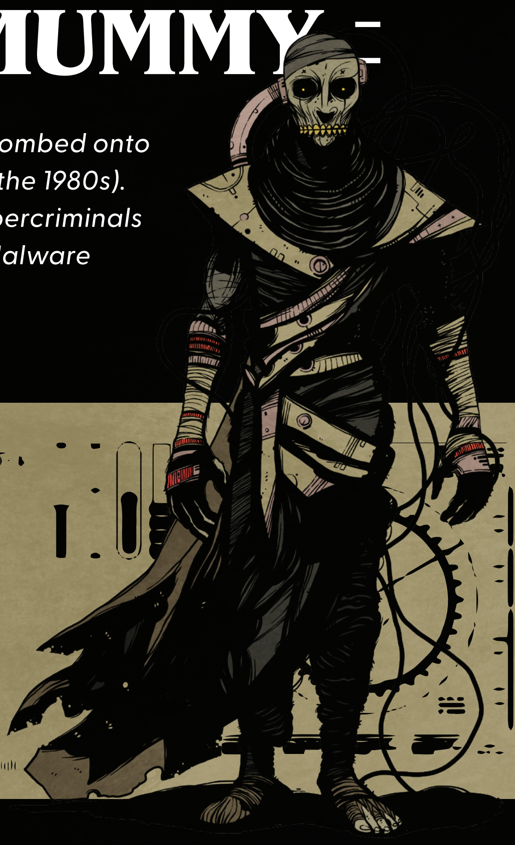
CLONE PHISHING:
Attack of the clones! Here, villains compromise email accounts, modify existing emails by replacing legitimate links or attachments with malicious ones and spread the infection to contacts.

MAN-IN-THE-MIDDLE ATTACK:
Eavesdroppers monitor communication between unsuspecting parties, often by creating fake public WiFi networks in public places.

RECENT VICTIMS

Phishenstein is a powerful beast, comprising nearly 22% of data breaches. Far from being a consumer malady, phishing attacks affect nearly 83% of companies.

THE MALWARE MUMMY



The last monster we're unraveling is the Malware Mummy, a terror untombed onto organizations and individuals since the beginning of time (or at least the 1980s). Short for malicious software, malware refers to intrusive software cybercriminals use to steal data or damage computers and computer systems. The Malware Mummy corrupts your computer network to cause mayhem and steal information for monetary gain or to sabotage the user.

RECENT VICTIMS

The Malware Mummy is not to be taken lightly, as 75% of U.S. organizations have experienced a malware activity that has spread from one employee to another. Over half a million bits of malware are detected daily, and in the first half of 2022 alone, there were 236.7 million ransomware attacks around the globe, at an average cost of $4.54 million per incident.

HOW MALWARE MUMMY STRIKES

The Malware Mummy attacks with all manner of creepy crawly things:

VIRUSES:
These cyber maladies attach themselves to documents or files supporting macros to spread from host to host. Once downloaded, they stay hidden in a dark corner until the file is opened like Pandora's box, disrupting system operations and causing data loss.

WORMS:
These malicious little software wigglies rapidly replicate and spread across devices within a network. As opposed to viruses, worms don't need host programs to spread and instead infect devices through downloaded files or network connections, with similarly disastrous results.

TROJAN VIRUSES:
Some gifts you don't want to accept, like a Trojan virus. These sneaky little snakes disguise themselves as useful software but instead get into sensitive data, modifying, blocking, or deleting it. While Trojan viruses do not self-replicate, they can still severely harm device performance.

SPYWARE:
These sneaky programs run in the shadows on your computer, reporting back to a remote user. They target sensitive information and can grant remote access to attackers, making it easy to steal financial or personal data.

FILELESS MALWARE:
The sneakiest of these is fileless malware, which operates from a computer's memory rather than files on the hard drive. This makes it especially difficult to detect and analyze.

WHEN CYBER MONSTERS *ATTACK*

The monsters of the cybercrime underworld are always on the prowl, ready to strike at unsuspecting organizations around the world. Some of their attacks have been particularly bad, causing costly damage and pauses in operations that had ripple effects to other industries and the world at large. Here are some of their most recent and heinous attacks:

The Ransomwarewolf sunk its teeth into the healthcare world when UnitedHealth-owned prescription processor Change Healthcare suffered a ransomware attack in February 2024, causing significant disruption in the U.S. healthcare system. A month after the attack, 80% of physician practices were still reporting lost revenue from unpaid claims, and 85% needed to allocate additional staff time and resources to complete revenue-related tasks.

In February 2024, a dark portal leading attackers into the heart of devices everywhere known as a zero-day vulnerability (a flaw within software hackers can take advantage of to steal data or implant malware) revealed itself within Ivanti VPN. This led to the recommendation that U.S. federal agencies such as Homeland Security and the Securities and Exchange Commission disconnect any devices using these VPN solutions within 48 hours. Globally, attackers compromised more than 2,000 devices.

In 2019, ZomBEC feasted on the Japanese company Toyota Boshoku Corporation, where cybercriminals stole $37 million by deceiving an employee into transferring the funds from the company's European subsidiary. Attackers stealthily exploited the company's large scale to make their request appear inconspicuous.

Of all of DOSula's dastardly deeds, one stands out from the pack: a 2017 attack on Google that reached a size of 2.54 Tbps, the largest attack of its kind. This DDoS attack saw the perpetrators send spoofed packets to 180,000 web servers, which sent responses to Google. Though the attack was akin to facing the biggest tidal wave on record, Google reported no disruptions to its service due to its preparation for such an attack, underscoring the importance of securing adequate cyberattack protection.

A big, hairy Phishenstein attack led to $100 million in damages to Facebook and Google between 2013 and 2015 when they paid fake invoices attackers sent to the companies on behalf of the Tawainese vendor Quanta, whom both companies used. Though the attackers were caught, Facebook and Google were only able to recover about half the stolen funds.

Sometimes, these beasts work hand in hand (or claw in claw?). This may have been the case when in 2021, Ransomwarewolf and Phishenstein seemed to team up against fuel supplier Colonial Pipeline.The organization was forced to pay $4.4 million in ransom and pause operations after attackers compromised its business networks and billing systems. This sent a ripple through the U.S. economy, as nearly half of the U.S. East Coast oil supply shut down for a week. As government reports say the DarkSide gang responsible for the attack commonly use phishing, it was likely the result of a phishing scam turned ransomware attack.

EVEN THE MOST DIABOLICAL MONSTERS HAVE *WEAKNESSES*

Luckily, the monsters of the cyber world aren't invincible. By targeting these beasts' weaknesses, you can transform yourself into a regular Van Helsing.

RANSOMWAREWOLF

Silver bullets against this beast include regularly backing up data to offline or cloud storage, and ensuring all software and systems are up to date with the latest security patches. Use robust antivirus and anti-ransomware tools to detect and block potential threats.

ZOMBEC

Cut ZomBEC off at the head before it gets its cold hands all over your data by implementing multifactor authentication (MFA) for email accounts, and train employees to recognize and report suspicious emails. Use email filtering and monitoring tools to detect unusual email patterns and unauthorized access.

DOSULA

Your string of garlic against DOS attacks includes reducing the attack surface into which it can sink its fangs by restricting traffic to a specific location, using a load balancer, and blocking traffic from unused apps, protocols, and ports. Use log monitoring to analyze unusual traffic patterns, a content delivery network (CDN) to cache resources and prevent them from being overloaded by real and malicious requests, and rate limiting to prevent web servers from getting overwhelmed by requests.

PHISHENSTEIN

To restrict the terrifying advance of phishing attacks, conduct regular cybersecurity awareness training for employees to recognize phishing attempts; utilize tools such as MFA, email filtering, and anti-phishing software; and foster a culture of skepticism towards unsolicited communication, encouraging recipients to report suspicious emails.

THE MALWARE MUMMY

Tips organizations and individuals can use to prevent malware from wrapping you in its grip include applying and adhering to policies and best practices for application, system, and appliance security; backing up your data; using next-generation endpoint monitoring tools; applying a zero-trust security framework; and education, education, education!

BOOST YOUR ARSENAL

The cybersecurity fight against threats is long and treacherous, but Pax8 is here to help! Think of us as your personal arsenal to battle the baddies of the cybercrime underground. Through the Pax8 Marketplace, you can provision the following weapons to help you protect your clients from the perils of these monsters run amok:

BACKUP AND DISASTER RECOVERY

These create copies of files, folders, and complete systems so they can be restored in case of emergency.

FIGHTS AGAINST: Ransomwarewolf

VENDORS:

Acronis
Arcserve
Axcient
Carbonite
Infrascale
Microsoft
Otava
Redstor
Symantec
Veeam

ENDPOINT DETECTION AND RESPONSE (EDR)

Endpoint security solutions continuously monitor end-user devices for cyber threats and contain them so security teams can remedy attacks before they take hold.

FIGHTS AGAINST: Ransomwarewolf, Malware Mummy

VENDORS:

Acronis
Bitdefender
CrowdStrike
Exium
SentinelOne
ThreatDown
Todyl
Trend Micro
WatchGuard

NETWORK SECURITY

Network security solutions protect networks from threats and unauthorized access.

FIGHTS AGAINST: DOSula, Phishenstein, Ransomwarewolf, Malware Mummy

VENDORS:

Exium
Perimeter81
Symantec
ThreatDown
Todyl
WatchGuard

DLP (DATA LOSS PREVENTION)

DLP helps you identify and prevent unsafe or inappropriate data sharing, transfer, or use across cloud and on-premises systems

FIGHTS AGAINST: DOSula, Phishenstein, Malware Mummy, Ransomwarewolf

VENDORS:

Acronis

EMAIL SECURITY

Email security solutions protect email accounts and messages from unauthorized access, loss, or compromise.

FIGHTS AGAINST: Malware Mummy, Phishenstein, Ransomwarewolf, ZomBEC

VENDORS:

Acronis
Avanan
Bitdefender
IRONSCALES
MailGuard 365
Microsoft
Perception Point
Proofpoint
Symantec
TitanHQ
Trend Micro
Vade

SIEM (SECURITY INFORMATION AND EVENT MANAGEMENT)

SIEM solutions continuously monitor and analyze security events and logs across an IT network.

FIGHTS AGAINST: Ransomwarewolf, Phishenstein, Malwarewolf, DOSula

VENDORS:

Blackpoint Cyber
Exium
Pillr
Todyl
WatchGuard

FIREWALLS

These prevent unwanted traffic from passing from one network to another.

FIGHTS AGAINST: DOSula

VENDORS:

Exium
WatchGuard

IDENTITY AND ACCESS MANAGEMENT (IAM)

IAM allows administrators to assign users with specific roles and permissions and control the resources they can access to prevent unlicensed access.

FIGHTS AGAINST: Phishenstein, Malware Mummy

VENDORS:

CyberFOX
Exium

POWERFUL PROTECTION *AGAINST* MONSTER ATTACKS

When it comes to battling foes of the cyber world, there's a lot to sort through. To create the antidote, get started by becoming a Pax8 partner. Our team of experts can help you plan and implement the best security stack for your clients, helping them keep the monsters at bay so they can focus on their core business – while you come through as their cybersecurity hero!

Get in touch, and you'll be well on your way to vanquishing the darkness lurking within the cyber world.

Become a Pax8 partner today!