
WHAT'S LURKING
in Your
SERVER CLOSET?
CYBER MONSTERS
VS.
YOUR HUMAN FIREWALL
UNITRENDS
A Kaseya COMPANY

For some, mistakes breed humility, but for the unfortunate, they're a one-way ticket to misery. Attention to detail is the name of the game, but should you waver, pray the monsters don't come out to play.

Welcome to the life of IT professionals. On the surface calm, cool and collected — masters of their domain. Yet, deep down, they know they are just one mistake away from letting cyber monsters have their way with an organization's IT infrastructure. IT pros are constantly looking over their shoulders thinking, *"what if I'm next?"*

Unfortunately, it's not a matter of if but when.

Would you believe that only 16% of businesses are adequately prepared to deal with cyberthreats?[1] It's a clear indicator that many IT pros and businesses are unaware of the proverbial monsters that aim to attack the weakest aspect of any business's data protection plan – their employees, or in other words, their "human firewall."

IT pros use everything in their arsenal, from a hodgepodge of business continuity and disaster recovery (BCDR) vendors to expensive security training sessions, to strengthen their organization's security posture. Yet, it's ultimately humans that are the primary cause of data loss.[2] This begs the question of what needs to be done to protect IT infrastructures from human fallibility as well as from server monsters that lurk in the dark, waiting for a mistake that gives them the perfect opportunity to strike.

This eBook aims to shed light on these monsters that lurk in your sever closet, luring employees into committing errors, wreaking havoc in your production environment, delaying strategic initiatives and causing major business losses. This eBook also provides solutions on how to bring an end to their reign of terror, allowing IT pros to concentrate on business growth as well as their career without worry.

The Ransombear

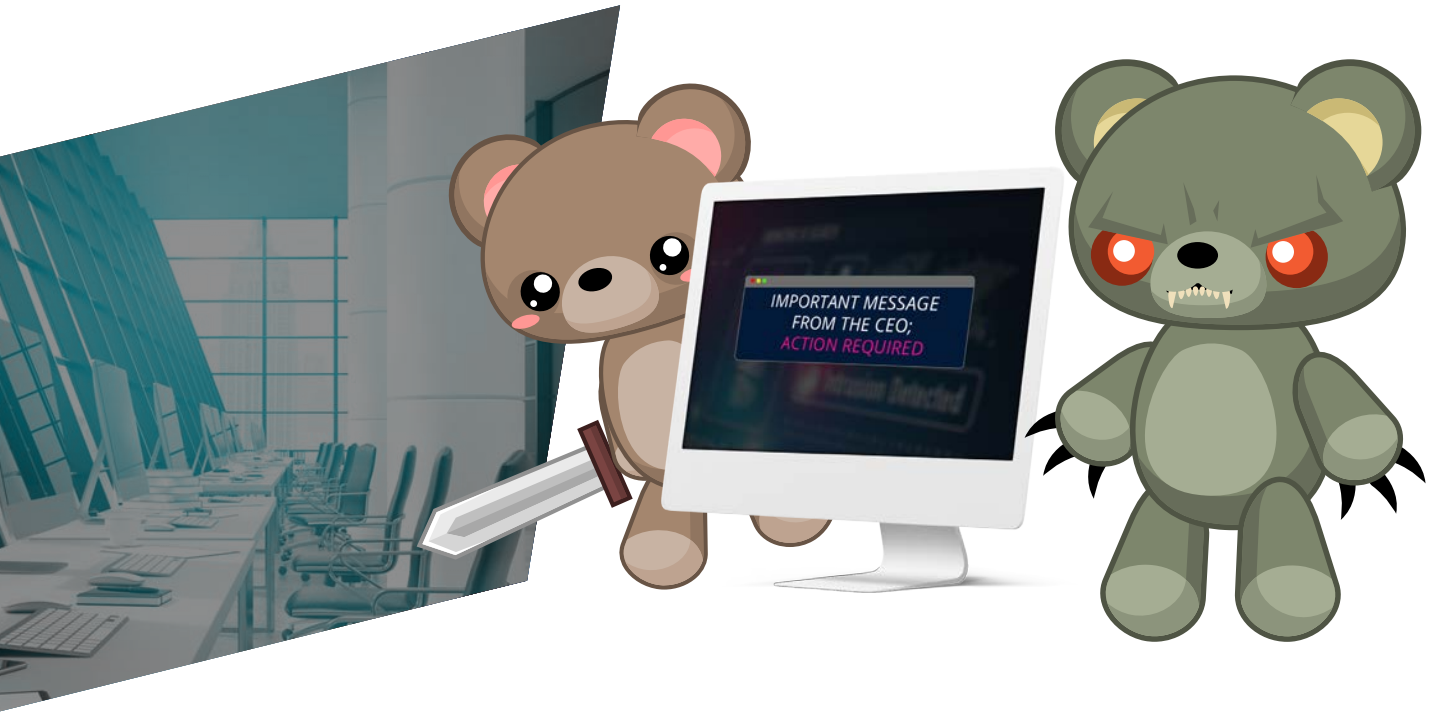
At first glance, the Ransombear appears friendly and innocent. However, with a single click, this impostor can detonate a payload that cripples systems, steals data and destroys businesses.

Cyberattacks have exploded in frequency, with phishing attacks being a primary delivery method. A whopping 65% of ransomware infections are delivered via phishing.[3]

In addition to phishing, cybercriminals see opportunities in keeping ransomware-causing-malware hidden within IT networks for long gestation periods to extract copious amounts of sensitive data, leading to a surge in advanced persistent threats (APT).

APT is a form of cyberattack through which a hacker gains and maintains unauthorized access and remains low key for a significant period. Attackers use the time between infection and remediation to monitor, intercept and turn over sensitive data. Stuxnet, an APT, took down Iran's nuclear program by traveling through USB sticks and Microsoft Windows computers until it destroyed the nuclear centrifuges.[4]

The average time to identify a breach is almost seven months or 207 days.[5] Attackers are finding smart ways to hide malware within IT networks to avoid detection.

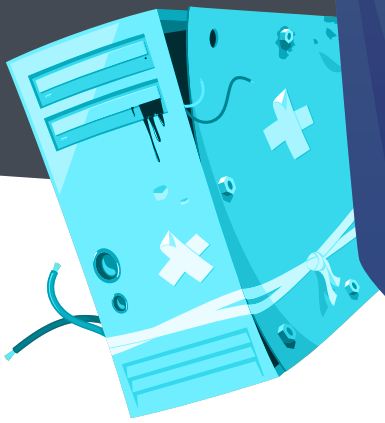


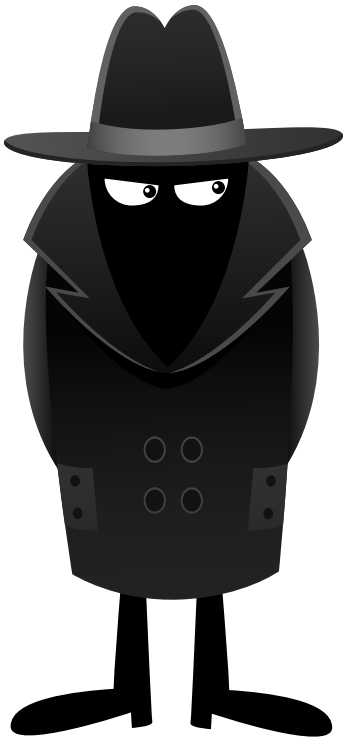
Here are some of the places malware loves to lurk:

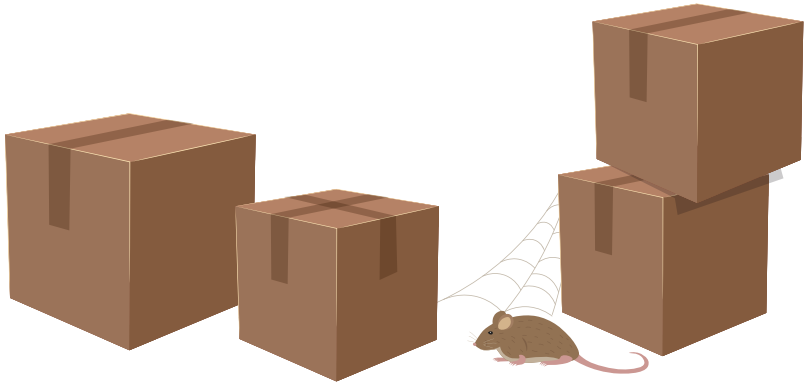
Windows Registry - Malware modifies Windows Registry keys to establish long-term residence within a network and further deploys more malware each time the OS is launched.

Temporary Folders - The loose security makes it a sweet landing page for ransomware after it enters the system.

.lnk Files - Both malware and ransomware can gain a foothold within a system after propped-up .lnk files that may resemble an existing shortcut, are downloaded.







The ATO Spider

The Account Takeover (ATO) Spider spins a web of deceit to gain access to user credentials. This eight-legged creature of the dark web tricks users into willingly giving away their logins and passwords before entrapping data across a company's network.

Phishing has grown exponentially and is now being used to gain access to account credentials. Account Takeover (ATO) attacks have increased at least 300% over the last two years, especially with the unprecedented rise in rookie remote employees working from home networks, often without the security of company firewalls and other safety measures.[6]

ATO attacks spring from cybercriminals stealing or buying credentials during third-party breaches and then reusing them to gain easy access to corporate systems to steal IPs, perpetrate business email compromise, gain access to financial accounts and commit other types of cyber fraud.

A whopping 80% of all businesses experience at least one compromised account threat per month.[7] IT pros know all too well that compromised accounts present a security loophole that can potentially wreck business reputation and consumer confidence.

Purge All Server Closet Monsters With Unitrends

Unitrends is your one-stop solution for conquering the cyber monsters that lurk in your server closet and take away your peace of mind. Protect data across physical data centers as well as virtual environments, cloud-native workloads and SaaS applications with ransomware detection, self-healing backups, dark web monitoring and much more.

Be Proactive With Ransomware Detection

Employ an all-out, multi-pronged approach of endpoint, network, server and backup level detection to protect data. Unitrends predictive analytics engines analyze backup data to determine the probability that ransomware malware is operating on a server, workstation or desktop computer. This also includes sleeper ransomware, where victims are unaware of its presence until the ransom demand appears. When ransomware conditions are proactively detected, it's easier to find the source of the threat. If infection is confirmed, IT pros can immediately restore systems from backups tested at the application services level to the last certified recovery point.

Test to Guarantee Fast Recovery

To achieve cyber resilience, regularly test recovery processes to ensure the business is prepared for an actual incident. Unitrends Recovery Assurance performs automatic testing to facilitate an assessment of the viability of the backup – including running trial recoveries up to the point of launching a backup application. This ensures backups are working and ransomware protection is effective. This gives 100% confidence you can meet Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs).

Security Integrations that Enable Proactive Defense and Reduce Frequency of Attacks

One of the greatest security investments an organization can make is one towards empowering their employees to take part in cyber defense. Spanning Backup for Microsoft 365 provides enterprise-class data protection for Microsoft 365 data, enabling restoration of files, folders, sites, and more. Purpose-built security integrations help organizations reduce the frequency and severity of data loss events. Phishing defense empowers IT and security teams to gain actionable insights into threats targeting their organization through investigation of alerts and autoquarantined emails, the export of real-time threat intelligence to your SEIM solution and visual cues for employees to alert IT to suspicious emails via automated workflows and feedback loops. Integrated dark web monitoring provides a more complete picture of your organization's security posture with proactive monitoring and alerting of compromised accounts and credentials which serve as early warning mechanism before a breach occurs.

Although you've learned all about the monsters that target end users by preying on employee behavior, they aren't the only ones out there. Learn about the monsters that enable data loss as we continue to combat IT pros' biggest nightmare.

Sleep easy knowing Unitrends keeps your data safe from the monsters lurking in your server closet

DOWNLOAD A FREE TRIAL

UNITRENDS
A Kaseya COMPANY

WP-2113-ENG-A

Sources

1. https://www.titanfile.com/blog/15-important-cybersecurity-statistics-in-2021/
2. https://www.grcworldforums.com/breaches-and-vulnerabilities/human-error-remains-the-main-cause-of-data-breaches/386.article
3. https://www.idagent.com/blog/whats-behind-the-huge-rise-in-healthcare-data-breaches/
4. https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-stuxnet.html
5. https://www.capita.com/sites/g/files/nginej146/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf
6. https://heimdalsecurity.com/blog/account-takeover-fraud/
7. https://spanning.com/resources/whitepapers/global-data-protection-survey-report-2016/