



RISK & RESILIENCE:


THE CYBER OPERATIVES



FIELD GUIDE

MISSION BACKGROUND

You may not be up against a villainous billionaire dangling you over a shark tank, but securing a modern business has more in common with the work of international superspies than you might think. The world of cybercrime can be just as dangerous, with equally lethal outcomes for business.

rganisations are increasingly reliant on cybersecurity professionals with the 007-level skills needed to take the best possible action when high level threats are in motion.

In every intelligence-driven operation, there's a "Q" who develops the essential tools of the trade. They lead ingenious teams to build and equip every field agent with just the right device, cipher, or solution to get out of dangerous situations and successfully complete their missions. An exploding pen or submarine car can make the difference between an agent that gets the living daylight's kicked out of them or that bounces back quickly to fight another day.

Your tools of the trade are less showy, but every bit as effective. When you're responsible for assessing, selecting, delivering, and servicing your customers' most critical systems, you need to be fully equipped to handle a diverse range of crisis-averting missions.

But technology will only get a newly suited Kingsman so far. 'Manners maketh man' refers of course to the critical importance of culture. For every trained professional following protocol in the cybersecurity field, there's a non-technical "civilian" that could accidentally trigger a ticking time bomb inside the business.

And right now, the timers on every threat are running faster than ever and the stakes are higher for everyone. The governmental powers-that-be are giving poorly protected, non-compliant and subsequently impacted businesses no quantum of solace when it comes to the size of penalties applied.

Resilience is the Main Character

The best secret agents are masters of the defensive arts. What's a good spy without a wicked roundhouse kick or an umbrella led parry after all? Likewise, powerful cyber defence is a critical element of a robust security strategy.

But what gives the good guys the real edge is a subtler, often under-sung characteristic: resilience. Without resilience – the ability to bounce back quickly and counter the next attack – our favourite characters wouldn't survive to make a sequel.

In our world, organisational cyber resilience is the equivalent of fighting off multiple assailants with a pen, then speeding down a ski slope avoiding machine gun fire and finally collaring the bad guys in the bowels of a burning building. All without getting a hair out of place. Resilience enables highly trained operatives to get up every day and do it again and again, with increasing success.

Cyber resilience ensures any operating environment has characteristics that are more Bond than Odd Job. After all, there's only so much protection available from a chunky bodyguard who can throw a hat but can't get up after a shock to the system.



**Reputation is what people think of you.
Character is what you are.**

– Orlando Oxford, *The King's Man* 2021

Nerves may be shaken but resolve is never stirred

Much like MI6, cyber resilience in a business is made up of your defensive capabilities combined with rapid-recovery disciplines and a committed, organisation-wide cultural mindset.

Of course, resilience is learned rather than earned, and usually as the result of experience gained on multiple missions. Each deployment into the field builds a stronger, faster, and ever-more adaptable organisation.

This document will not explode once you have finished reading it, but the information it contains could help you to identify and remediate ticking time bombs in the tech environments you manage.

Your missions – and you are advised to accept them – follow.

FOR YOUR EYES ONLY:

MISSION CASE NOTES



Hello Partner Agent,

To assist you in your mission to reduce risk and build resilience within your operational domains, Crayon Headquarters has compiled prior case notes across four top-secret areas: Data, Identity, End Point, and Platforms. Use these to gain more insight to the techniques, tactics, and procedures of your adversaries.

Your mission briefing notes include updated guidance on how to mitigate the weakest link in the most organisations – human behaviour. Poor organisational culture will eat your security strategy for breakfast, so make the most of this essential advice.

With the right skills, technology, and an ongoing commitment to consistently progress resilience measures, your mission team will be more than a match for the wicked plans of threat operatives.

As usual, should you need additional assistance in the field, **Crayon Headquarters** will be standing by.



Stopping the bad guys ... that's what I do.

— Jack Bauer
On Her Majesty's Secret Service (1969)

TOP SECRET: MISSION OPERATIVES

MISSION TEAMS ▼

ENEMY OPERATIVES ▼

DATA MISSION	 <div>PARTNER OPERATIVE</div> <div>IZZY SALANDER</div> <div>Highly skilled in system monitoring. An expert in anomaly identification.</div>	 <div>K@TF15H3D!</div> <div>Social engineering racketeer. Uses ONIT (open-source intelligence) to crawl company social media feeds and websites to identify potential targets.</div>
	 <div>ALLIED OPERATIVE</div> <div>MICHAEL BLOMQUIST</div> <div>Owner of online florist, Blommie's Blooms. Runs a cloud-based procurement platform for transacting with suppliers.</div>	
IDENTITY MISSION	 <div>PARTNER OPERATIVE</div> <div>MIRACLE MAX</div> <div>Cybersecurity consultant, subject-matter expert in identity governance.</div>	 <div>H4CKPIC30N</div> <div>Hacker for hire. Never sleeps. Exists on Red Bull, chocolate-coated coffee beans and the thrill of illicit financial gain.</div>
	 <div>ALLIED OPERATIVE</div> <div>LAST RESORT</div> <div>IAM Analyst in Leap2Coin, a medium-sized financial services company that operates in three Asia-Pacific countries.</div>	
END POINT MISSION	 <div>PARTNER OPERATIVE</div> <div>LETHAL WEAPON</div> <div>Skilled engineer who manages user workstations and servers on behalf of allied operative organisations.</div>	 <div>UNC6662</div> <div>Sponsored hacker group. Works in tightly coordinated sprints to rapidly exploit announced vendor vulnerabilities.</div>
	 <div>ALLIED OPERATIVE</div> <div>MURTAGH</div> <div>IT Manager of Priory Group Labs, a life sciences R&D business. Runs shared services for 20 labs across the region.</div>	
PLATFORM MISSION	 <div>PARTNER OPERATIVE</div> <div>O'BRIEN</div> <div>Analyst at CommerSec, an MSP that specialises in the e-commerce sector. Deep knowledge of cloud platforms, systems and programs.</div>	 <div>KR@5HK@RTB@ND1K00T</div> <div>Threat actor that executes attacks on e-Commerce platforms and website payment pages.</div>
	 <div>ALLIED OPERATIVE</div> <div>RUBIN</div> <div>Founder of RevGen, a digital agency that develops back-end and front-end e-commerce properties.</div>	



MISSION 1

ELIMINATE INVASIVE WEED FROM THE TRANSACTION DATA GARDEN

— — — —



Data is the most valuable asset in the digital age. It can bring governments to their knees or empower those who possess it. In the wrong hands, it's a weapon of mass disruption.

— Ethan Hunt, Mission Impossible



MISSION ALERT

AGENT ALERT: New chatter received. Increased activity detected from threat actor K@tF15h3D! Field agents deployed within online retail cyber-arenas are advised to be vigilant.

TACTICAL RISKS

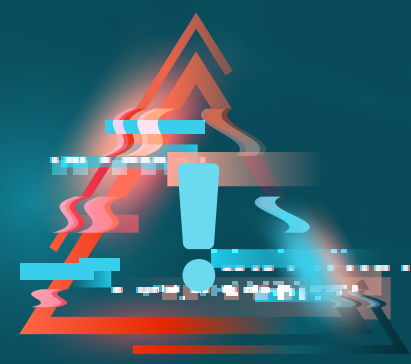
Social reconnaissance and pretexting are common tactics for bad agents. Information readily available on public forums using simple open-source intelligence tactics (OSINT) are used to gather data on organisations and their employees in order to create a false persona, which is then used to lure employees into additional communication.

Attackers are patient and will invest time into establishing rapport – essentially catfishing employees.

After building a dialogue and maintaining the false persona pretext for some time, attackers will lean into the relationship, spear-phishing individuals to gain what they need to access company systems.



ATTACK SCENARIO



A large digital advertising campaign and a successful PR drive about the flourishing growth of Blommie’s Blooms catches the attention of K@tF15h3D!

A quick search online turns up a recent event highlighted on the company social media page, and a post thanking Blommie’s major suppliers for their support. Supplier company names and individuals are tagged in the post.

K@tF15h3D! sifts through the supplier websites and social channels. After spotting a senior executive without a social media profile, the threat actor quickly sets up a false online identity.

OPERATIVES' GO BAG



Essential Field Manoeuvres

- Operatives trained to execute the following:
- **Data auditing:** maintain visibility of changes to permissions and access controls
 - **Reporting:** accurate records of who accesses sensitive data
 - **Analysis:** ability to identify behavioural anomalies based on audit data

Critical Technical Countermeasures

- DNS Filter
- Identity Access Management
- Multifactor Authentication
- Domain Based Message Authentication Reporting and Conformance

ATTACK SEQUENCE



Connection requests are issued to 20 staff members tagged in photos from the event. Details observed from the company social media post are used to create believable pretext.

“Hi [name], it’s James from Rosebury Rose Wholesale. Finally decided to get myself onto the socials! Hahah! Had a great time at the event on Thursday night, really love O Bar, it’s a fantastic venue and such a great view! Enjoyed meeting you, Anna and the rest of the team from Blommies. Looking forward to connecting with you all again soon.”

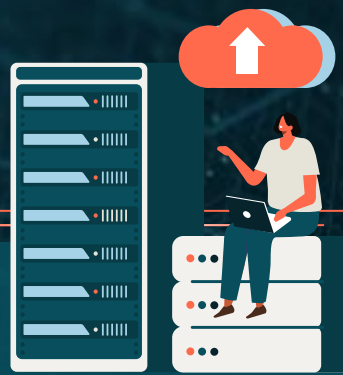
Half the staff members accept the connection. K@tF15h3D! sets about establishing chat conversations with each staff member managing to extract information around internal systems used.

Leveraging newly acquired information K@tF15h3D! is able to create a false malicious site to mimic the supplier portal.



14% OF SURVEYED ORGANISATIONS HAVE CURRENTLY ADOPTED MANAGED DETECTION AND RESPONSE, WITH A FURTHER 39% INTENDING TO ADOPT BY 2025.¹

CASE FILE



Izzy Salandar works for Blommie’s cloud service provider. She monitors data across managed cloud environments and services, including intercompany data exchanged as part of supply chain transactions.

Monday mornings usually see a large number of logins to Blommie’s supplier portal, but today Izzy notices an odd lull. She maintains watch and soon becomes sure there is an anomaly. The owner of Blommie’s, Michael Blomquist, is alerted.

Blomquist contacts one of his suppliers and is told they received an email and attached document that appear to be from Blommie’s Blooms. Written on Blommie’s letterhead, the document provides instructions to update login details to the supplier portal using a new link. The letter contains specific information about the supplier’s recent transactions on the portal, giving them little reason to doubt the authenticity of the request.

Izzy quickly investigates to find the link in the forged document leads to a sophisticated sham site that looks exactly like the interface for the genuine supplier portal.

Izzy suspects an attacker may be using harvested details to login to the real portal.

CASE REPORT

Field Agent Actions Taken

IDENTIFY & CONFIRM

Izzy establishes an around-the-clock watch on the portal. Just after midnight, several suppliers appear to login with their credentials. New invoices are submitted with banking details that have only minor variations from the suppliers’ genuine transaction accounts.

ISOLATE

Having confirmed an attack sequence is underway, Izzy segregates the compromised cloud portal from the network and other resources. She revokes access privileges for all users to prevent any further unauthorised activity.

ENACT

All compromised credentials are changed including passwords and API tokens.

INVESTIGATE

A review of all company interactions with the supply base identifies several new connections made via a business networking social media site. Soon, this is identified as the source of a spear phishing attack that resulted in K@tF15h3D! gaining access to the supplier portal. The email domain of the company was spoofed and used to issue the first contact to suppliers. Gaps in domain-based message authentication and a lack of multifactor authentication on the email messaging platform and portal login contributed to the incident.

CURRENT STATUS

Izzy’s eagle-eyed monitoring of anomalies prevented the potential payment of fake invoices totalling \$115,000 into bank accounts set up by the attacker. This monetary loss would have put Blommie’s Blooms at significant risk of not being able to pay legitimate invoices from its suppliers. All suppliers were advised that banking details may be compromised and were provided with full support to take the relevant precautions needed to avoid any further exploitation.

RECOMMENDED RESILIENCE MISSION EXTENSION

- ✔ Implement DMARC to a reject level.
- ✔ Initiate multi-factor authentication on email messaging platform and portal.
- ✔ Implement attribute-based access to the portal.
- ✔ Implement DNS filtering to block access to suspicious domains.



*The Future of Operations: Maximise the Value of Cloud with a Strategic Mindset, a Forrester Consulting study commissioned by rhiipe, December 2022.



MISSION 2

COUNTER ATTEMPTS TO GAIN PRIVILEGE USER IDENTITY

— — — —



We need to fortify our systems, implement strong access controls, and monitor for any suspicious activity. Our mission is to keep them out and protect our sensitive information at all costs.

— Harold Finch, Person of Interest



MISSION ALERT

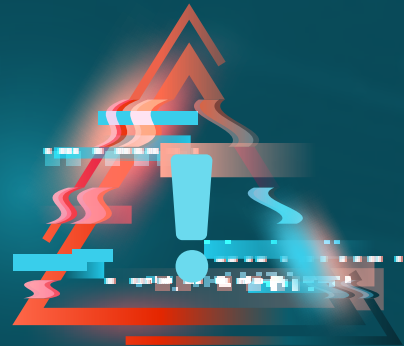
Incoming transmission ... Echo Level Alert ...
H4ckP!g30n is at large ... LDAP server reconnaissance activity indicated with concentration in financial sector arena. Priority order issued to identify and mitigate any exposure, stat.

TACTICAL RISKS

Internet facing portals / applications that allow end users to authenticate against internal systems using network credentials can often leave organisations exposed. Cracking open an LDAP server will allow unauthorised access to a trove of organisational data including directory structures, departments, groups, insights into the internal network, usernames, APIs and potential targets. In short, a successful attack will provide a roadmap that can be used to identify users, and privileged access levels, and then fine tune an attack to take over those privileges.

How does it happen? Accidental exposure of LDAP servers to the internet can occur because of server misconfiguration and security vulnerabilities. Bad agents can use a range of tactics to scan for exposed LDAP servers, using specialised search engines and automated tools to identify open ports on target systems. Known vulnerabilities can be exploited using vulnerability scanners or scripts to automate the process.

ATTACK SCENARIO



Using a combination of nMap, Google Dorking, Shodan and automated vulnerability scanning scripts, H4ckP!g30n identifies a vulnerability which allowed them to anonymously query internal LDAP server used by Leap2Coin for authenticating a cloud trading platform application.

ATTACK SEQUENCE

1. Leveraging a known vulnerability identified on external system which was exploited allowing for LDAP queries to be executed against internal directory.
2. A carefully crafted query was run to identify all user memberships of known privileged groups.
3. List of users were then dumped into a text file ready to be used in an automated script against a dictionary of known breached passwords.
4. Attack strategy: dictionary attack using password spraying.



OPERATIVES' GO BAG



Essential Field Manoeuvres

- **Audit and discovery:** scope the mission ahead with audit of all domain objects, rights and permissions
- **Analysis:** determine actions that objects can perform and strength of credentials at client site / minimise attack surface actions by addressing highest risks first
- **Harden:** ensure users only have access required to perform necessary tasks within their roles
- **Enforce:** secure communication protocols (TLS/SSL).

Critical Technical Countermeasures

- Active Directory Auditing, Monitoring and Defence
- IAM: management of user identities access privileges (privilege access management) and authentication processes. Enforcement of strong password policies, support for multi-factor authentication, centralised user provisioning and deprovisioning
- Web Application Firewall
- Vulnerability testing: scanning and assessment of LDAP infrastructure for weaknesses, known vulnerabilities and misconfiguration.

OVER 80% OF BREACHES INVOLVE BRUTE FORCE OR THE USE OF LOST OR STOLEN CREDENTIALS.² UNPATCHED SOFTWARE IS A KEY VULNERABILITY IN SUCH ATTACKS.³

CASE FILE

Last Resort, an IAM Analyst at Leap2Coin, woke Monday morning to see an alert blinking on his phone. His company was subject to an unknown intrusion while he slept.

Investigating immediately, Last Resort identified a series of failed logon alerts across multiple internal IPs. The company's threat detection and response platform pinpoints the targets: all affected user accounts belong to helpdesk admins.

Luckily, there's an incident response plan already in place and the alarm is raised to the wider team without delay.

With the immediate response underway, Last Resort knows he'll need expert advice to prevent further exploitation of Leap2Coin's platforms. He's going to need Miracle Max.



CASE REPORT

Field Agent Actions Taken

INVESTIGATE

Active directory threat investigation reporting tool initiated to investigate the password spray attack. Exposure on LDAP server tracked back to a combination of poor configuration of both the web application and the web application firewall.

IDENTIFY & CONFIRM

Miracle Max and Last Resort commence a review of audit logs related to out-of-hours domain activity. They detect LDAP reconnaissance utilised by threat actor H4ckP!g3on and confirmation that the threat agent successfully identified a list of all known user accounts in the Leap2Coin directory.

ENACT

- All affected accounts are immediately disabled.
- Password reset solution is deployed across all Active Directory user objects.
- Event is reported to relevant authorities.

CURRENT STATUS

Working together, Miracle Max and Last Resort were more than a match for H4ckP!g3on's password spray efforts. The existing zero-standing-privilege foundation ensured all privilege was gated behind multi-factor authentication and automated provisioning of admin user accounts. In addition, their fast action with credentials deletion has meant no successful authentication by the threat agent.

This winning strategy ensured 100% of Leap2Coin's company and customer data was secured. However, there is work to be done to advance counter measures against similar tactics in future.

RECOMMENDED RESILIENCE MISSION EXTENSION

- 🕒 Implement full web application vulnerability regime



² <https://enterprise.verizon.com/resources/reports/dbir/>

³ <https://thehackernews.com/2023/03/lastpass-hack-engineers-failure-to.html>



MISSION 3

PREVENT EXPLOIT OF END POINT SECURITY VULNERABILITIES

— — — —



The greatest weapon against an end-point attack is not a gadget or a firearm, but knowledge. Know your enemy, know your system, and anticipate their every move.

— Jack Bauer, 24



MISSION ALERT

OMEGA LEVEL ALERT ... Intelligence reports have detected increased activity from state-sponsored groups targeting recently identified vulnerabilities in IP-PBX desktop clients and remote management software.

Detected TTPs indicate paid espionage and ransomware-as-a-service attack motivators.

HQ and Allied operations are both at risk.

CODE RED: Field offices should immediately identify any use of vulnerable platforms and systems. Remediate with extreme prejudice to eliminate burrow-through risk to Allied environments.

EXTREME PRECAUTION PROTOCOLS: Proactive manoeuvres mandated for field operatives deployed in high- value intellectual property sectors.

TACTICAL RISKS

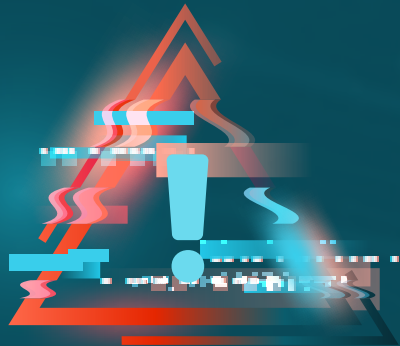
Endpoints provide a gateway to all company data. Successfully installing malware on desktops, laptops, mobile devices, or servers is the most common means for threat actors to capture application data and follow up with a ransomware attack.

Tactics include “juice jacking” which lays malware install traps by modifying ports in public charging stations commonly found in airports, commuter transit hubs and industry events.

End point attacks are not limited to the big end of town. 47% of SMBs (100 – 1,000 employees) have now experienced a ransomware attack. Threat actors exploit the fact that smaller businesses are less likely to have dedicated security resources and systems customer arena.

Threat actors also target Managed Service Providers, seeking to ‘access one, attack many’ by gaining access to MSP systems and burrowing through into customer environments.

ATTACK SCENARIO



Hacking group UNC6662 is targeting boutique laboratories – and their service providers – seeking to exfiltrate and ransom high-value intellectual property.

1. **External reconnaissance:** UNC6662 scans for open ports and potential exploits of known vulnerabilities in IP-PBX desktop application and in remote management software.
2. **Initial compromise:** multiple unpatched authentication bypass vulnerabilities and misconfigurations are exploited. An initial payload is delivered to facilitate internal reconnaissance.
3. **Internal reconnaissance:** gathering information on existing accounts, privileges and access.
4. **Lateral movement:** Deploy tactics to take over internal accounts and gain access to privilege environments.
5. **Escalate privileges:** privileged command access gained via misconfigured access control lists. Modified request parameters used to bypass authentication mechanisms.
6. **Deliver payload:** malware upload initiated.
7. **Establish persistence:** backdoors created via modified system files and registry entries.

ATTACK SEQUENCE



OPERATIVES' GO BAG



Essential Field Manoeuvres:

- **Patch Management:** evaluate patches based on potential impact of attack on business continuity. Prioritise for operating systems, software and applications commonly targeted by attackers or known to have vulnerabilities. Review potential impact on systems and data.
- **System Monitoring:** track the patch status of systems and proactively remediate where critical patches are missing.
- **Log review and threat identification**

Critical Technical Countermeasures:

- Application Allowlisting
- Endpoint Detection and Response solutions
- Endpoint Protection Platforms
- Local Security Authority Subsystem Service Monitoring and Blocking.

57% OF SURVEYED ORGANISATIONS CURRENTLY HAVE ADOPTED ENDPOINT SECURITY SOLUTIONS, WITH 34% INTENDING TO ADOPT BY 2025.⁴

CASE FILE

Priory Group utilises an IP-PBX desktop application to enable all onsite, hybrid and remote users with access to the company VoIP system.

The desktop application is a tempting attack surface, but it isn't unprotected. Over at Rapid Fire Cloud Services, field agent Lethal Weapon routinely uses a widely adopted remote monitoring and management software solution to administer endpoint workstations, desktops, and laptop devices for Priory Group.

Lethal Weapon receives alerts from HQ and vendors regarding identified vulnerabilities in both solution sets. Recognising the potential for a supply chain attack, she places a call to allied operative, Murtagh at Priory Group. A proactive plan is enacted to implement an application Allowlisting solution across both organisations, in addition to the existing EDR.



CASE REPORT

Field Agent Actions Taken

SCOPE

Endpoints, operating systems, and applications to be covered with Allowlisting solution for Rapid Fire and Priory Group.

IDENTITY

Authorised applications and needs of different user roles across Rapid Fire and Priory Group to ensure all necessary applications are included.

SET POLICY

Define criteria for including applications in the Allowlist. Set rules for application updates and version control to ensure only approved and up-to-date versions are allowed to execute.

CONFIGURE

Enforce Allowlist policies to prevent execution of unauthorised or untrusted software.

CURRENT STATUS

Murtagh and Lethal's proactive solution implementation has mitigated potential endpoint and script exploits.

Out-of-date, unpatched, or unapproved versions of files are no longer able to run. An explicit block rule prevents the execution of any compromised MSI file to prevent auto-updates of endpoints to any malicious versions.

Unauthorised or unapproved software blocked from install on endpoints.

Execution of untrusted script including any attempts to deliver via malicious documents or attachments is blocked. Malware and ransomware infections blocked from execution.

RECOMMENDED RESILIENCE MISSION EXTENSION

- ✓ LSAS monitoring and blocking
- ✓ Create supplier policy to ensure alignment to required security standards
- ✓ Review of patch management processes
- ✓ Review DNS filtering capability to ensure inbound and outbound calls
- ✓ Implement constant review of EDR efficacy



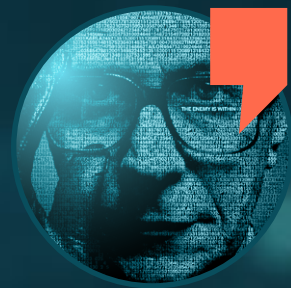
⁴ The Future of Operations: Maximise the Value of Cloud with a Strategic Mindset, a Forrester Consulting study commissioned by rhipe, December 2022



MISSION 4

DENY ENEMY ACCESS TO PLATFORMS

— — — —



Our mission: protect the cloud, preserve the secrets, and outmanoeuvre the enemy.

— Tinker Tailor Soldier Spy

MISSION ALERT

BATTLESTATION UPGRADE WARNING! Operation Cashcard has confirmed a surge in darkweb chatter around Black Friday. Hypervigilance on Magecart TTPs on browser and server side is advised. Watch for signs of malicious code injections, compromised third-party services or encrypted appendages on regular server images. Operatives should immediately advise all allies utilising Magento, WooCommerce, Adobe Commerce, and other commonly utilised platforms. PATCH! PATCH! PATCH!

TACTICAL RISKS

Magecart has become a ubiquitous term for digital skimming attacks targeting vulnerabilities in e-commerce platforms and web browsers to exfiltrate credit card details for sale on the dark web.

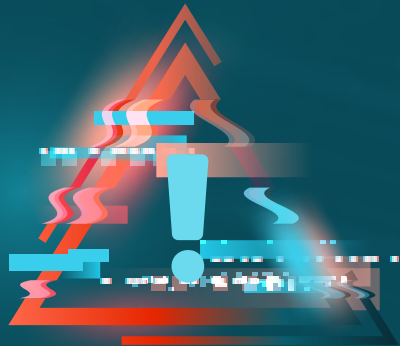
Attackers are adept at automating scans of the web, seeking outdated e-commerce sites and vulnerable plug-ins. When enacted on browsers, malware is injected into e-commerce payment pages and malicious script captures data entered to payment forms. This kind of attack does not affect the transaction itself, so is often harder to detect.

The holy grail for threat agents is attacking on the server-side to execute a supply chain compromise. There are many techniques used in such attempts, which attack third party scripts, libraries, or plugins. When successful, the compromised website server loads malicious code that has been injected into legitimate resources, such as Google Tag Manager containers to capture card payment details.

Persistence levels are amongst the highest of all attack types, with one out of five eCommerce websites compromised by a Magecart attack re-infected within a matter of days. Threat agents set up multiple backdoors, rogue admin accounts, hidden periodic tasks and database triggers as means to re-install malicious code in the event it is detected and removed by system admins.

Smaller businesses are at increased risk, especially since the COVID-era mass migration to e-commerce solutions.

ATTACK SCENARIO



Threat actor Kr@5hK@rtB@nd1Koot uses trojanised Google Tag Manager (GTM) containers to execute Magecart attacks on e-Commerce platforms and website payment pages.

ATTACK SEQUENCE

1. Reconnaissance: scan known Black Friday participant websites for GTM containers used to manage tracking and analytics scripts.
2. Build knowledge base of site structure, GTM implementation and specific tags in use.
3. Compromise point identified in Crazy Egg analytics script using injection of blended code and modified container config. Confirm browser execution.
4. Process data harvesting, encrypt exfiltrated payload and transmit.



OPERATIVES' GO BAG



Essential Field Manoeuvres

Web Application Security knowledge: XSS, SQL injection and insecure direct object references

Secure Coding: fundamentals of JavaScript, Python, PHP

WAF: ability to deploy and configure Web Application Firewall solutions and rulesets

Cloud Security Assessments: Proficiency in security testing techniques

Critical Technical Countermeasures

- **Dynamic Application Security Testing tools:** scan web applications for known security vulnerabilities, detection of code level vulnerabilities, injection detection, analysis of security header effectiveness, assessment of web applications against compliance standards.
- **Privilege Access Management solution:** enforcement of least-privilege principle, tracking of privilege user actions, audit trailing, Just-in-Time access to prevent continuous access to sensitive systems, session monitoring and recording, strong password management, support for 2FA and MFA.
- **ZTNA:** strong identity verification for resource access, limited access rights to prevent lateral movement, micro segmentation of network and isolation of sensitive resource, application-centric access, continuous monitoring and behavioural analytics, integration with Secure Web Gateways for real time inspection and filtering of web traffic.
- **Cloud Access Security Broker:** visibility into cloud applications and services in use, identification and monitoring of third-party scripts.
- **Application Allowlisting:** Control which files can be executed on endpoints and block non trusted. Preventing the execution and spread of malicious code.
- **Automated Patch Management:** Ensuring all applications and Operating systems are fully up to date preventing known vulnerability exposure.
- **Assess and Manage third party risk:** Commercial software provides threat actors a vector to hide and distribute malicious artifacts to thousands of unsuspecting enterprises and government agencies. Automating scanning of third parties to identify vulnerable assemblies hidden applications assist in mitigating risk of third-party supply chain attacks.



36% OF SURVEYED SMBS IN APAC HAVE CURRENTLY IMPLEMENTED CLOUD WORKLOAD PROTECTION PLATFORMS, WITH A FURTHER 34% INTENDING TO ADOPT BY 2025.5 (FORRESTER/RHIPE FUTURE OF OPERATIONS).

CASE FILE

Allied operative Rubin is the founder and CEO of RevGen, a fast-growing digital service agency specialising in front-end and back-end e-commerce site development for customers in retail, travel, hospitality, and entertainment sectors.

He has seen news articles about cybersecurity risks associated with Google Tag Manager containers, which RevGen uses to track and manage activity across its customers' websites and applications.

Rubin assembles a dedicated team of developers, project managers and IT staff together with O'Brien from their MSSP, CommerSec, to determine the level of risk and ensure rapid mitigation.



CASE REPORT

Field Agent Actions Taken

- 1. Proactive response:** prioritize the identification, assessment, and mitigation of risks related to trojanised GTM containers to protect clients' businesses.
- 2. Client communication:** The agency proactively reaches out to its clients, informing them about the potential risk of magecart attacks through trojanised GTM containers. They explain the measures being taken to address the issue, assure clients of their commitment to security, and recommend necessary actions to safeguard their e-commerce platforms.
- 3. Internal assessment:** O'Brien conducts an internal assessment of existing projects, focusing on the usage of GTM containers. He identifies websites and applications that leverage GTM and evaluates the potential vulnerabilities and risks associated with these implementations.
- 4. Container validation and security review:** Thorough examination of each GTM container used in agency projects to validate the integrity of the containers, ensuring they have not been compromised or tampered with. Review of the security measures in place, such as container permissions, access controls, and monitoring mechanisms.
- 5. Security enhancements:** O'Brien works closely with the agency development team to enhance the security of GTM containers and associated code. They implement additional security layers, including input validation, output encoding, and secure coding practices, to mitigate the risk of malicious code injection.
- 6. Backup enhancements:** Increase frequency, scanning and testing of scheduled backups to offsite storage and backup verification to ensure web platforms and data can be recovered.
- 7. Continuous monitoring:** O'Brien deploys real-time monitoring and logging mechanisms to detect any unauthorized changes or suspicious activities within GTM containers. He sets up alerts and notifications to promptly respond to any signs of compromise or potential magecart attacks.
- 8. Supply chain risk mitigation:** Thorough assessments of third-party vendors are initiated, including GTM container providers and other service providers involved in RevGen's projects. Security practices, vulnerability management processes, and adherence to industry standards to ensure a secure supply chain.
- 9. Incident response and recovery review:** revise the established incident response and recovery plans to define processes and policies related to magecart attacks.
- 10. Ongoing Security Maintenance:** The agency extends the services agreement with CommerSec to include regular review and update of GTM containers, patches and security fixes.

MEMO TO HQ

Level 3 Resilience Parameters Achieved

- ✓ Proactive measures and stepped-up monitoring of the GTM threat vector paid dividends. RevGen is operating a Level 3 resilient environment, which is required to withstand the magecart attack tactics deployed against the business.
- ✓ Attack attempts on fifteen of RevGens' hosted customer sites commenced 24 hours before Black Friday, and to date, there is no evidence of any success.
- ✓ RevGen's customers transacted more than \$32 million during the Black Friday sales, which would have hauled a phenomenal payload for the threat agent if we had not put these measures in place. The fallout for RevGen would have been enough to shutter the business. Chalk another one up for the good guys!

⁵ Future of Operations: Maximize the Value of Cloud with a Strategic Mindset, a Forrester Consulting study commissioned by rhipe, December 2022

ADVISORY UPDATE:

CULTURE IS KEY TO THE SUCCESS OF EVERY RESILIENCE MISSION



Sometimes the enemy isn't lurking in the shadows or hiding behind sophisticated technology..... a weak company culture, riddled with complacency and carelessness, becomes the greatest vulnerability. Remember, the enemy can exploit not just systems but people. Guard against the insider threat and let loyalty to the mission prevail.

— John Clark, Without Remorse

A poor cybersecurity culture leaves a back door open to malicious outsiders who will take advantage of any opportunity to find your weakest link. Human behaviour has the potential to render even the most comprehensive cyber resilience strategy worthless. IBM researchers found that negligence caused 63% of incidents, well above the threat of criminal insiders at 14%¹.

Traditional security solutions like firewalls and other mechanisms are typically outward-focused and may not pick up internal threats such as an authorised login being used by the wrong person.

Field operatives must create a cyber-resilient culture to raise security awareness. All members of the team – with a particular focus on those handling payments – should be aware of cybersecurity risks, have a sense of ownership and accountability for security in their role, know how to spot potential risks, knowledge of emerging threats, a willingness to report suspected risks, and know what to do if/when they realise they have made a mistake.

Operatives can assess the organisation's security culture through ad-hoc discussions, formal surveys, and test drills such as fake phishing emails to identify careless team members who click on links. Gaps can then be addressed through ongoing training and reminders.

POOR CULTURE SIGNAL ALERTS

Signs of a poor cybersecurity culture in your team include:

- An attitude among staff that cybersecurity is “not my problem” and is the IT team’s responsibility.
- High prevalence of shadow IT, or apps downloaded without permission.
- Weak passwords in use or a complacent attitude towards password management.
- Poor education and awareness of common cybercriminal tactics such as scams, phishing emails or malicious links that will infect the system with malware.
- Devices frequently left exposed and unsecured.
- Employees who work around or evade “inconvenient” security measures.
- A willingness to ignore security policy and process.

¹ <https://www.ibm.com/security/digital-assets/services/cost-of-insider-threats/#/>

RESILIENT ATTRIBUTES

- **Security Awareness:** Employees have a deep understanding of cybersecurity risks, best practices, and the importance of their role in maintaining a secure environment. Culture reviews are scheduled and use interviews, surveys, and test drills to ensure security corners are not cut.
- **Proactive Mindset:** The organisation fosters a proactive approach to identifying and addressing cyber threats, rather than reacting after an incident occurs.
- **Collaboration and Communication:** Teams and departments collaborate and communicate effectively, sharing information, knowledge, and insights related to cybersecurity. Businesses are committed to retaining the operational flexibility needed to support growth and speed-to-market, without creating cybersecurity risk.
- **Continuous Learning:** There is a commitment to ongoing learning and development in cybersecurity, staying up-to-date with emerging threats, technologies, and industry best practices.
- **Ownership and Accountability:** Employees take personal responsibility for cybersecurity, understanding the impact of their actions on the organisation's security posture.
- **Risk Management:** The organisation has a risk-focused mindset, conducting regular risk assessments, implementing controls, and prioritising risk mitigation.
- **Incident Response Readiness:** There is preparedness to detect, respond, and recover from cybersecurity incidents through well-defined incident response plans and regular drills.
- **Executive Leadership Support:** Leadership champions and supports cybersecurity initiatives, allocating resources, setting the tone, and making cybersecurity a strategic priority.
- **Employee Empowerment:** Employees are empowered to report security incidents, voice concerns, and actively contribute to improving cybersecurity practices.
- **Resilient Infrastructure:** The organisation invests in robust cybersecurity technologies, tools, and infrastructure to detect, prevent, and respond to threats effectively.
- **Compliance and Governance:** Compliance with relevant regulations, standards, and industry best practices is prioritised, ensuring a strong governance framework.
- **Continuous Improvement:** The organisation plans progressive investment to introduce additional measures as needed.

16% OF SMBS CURRENTLY EMPLOY USER AND ENTITY BEHAVIOUR ANALYTICS, WITH A FURTHER 39% INDENTING TO ADOPT BY 2025.6 (FORRESTER/RHIPE FUTURE OF OPERATIONS)

⁶ Future of Operations: Maximize the Value of Cloud with a Strategic Mindset, a Forrester Consulting study commissioned by rhipe, December 2022



LOOKING FOR AGENTS WITH THE TRAINING AND EXPERTISE NEEDED TO ACCOMPLISH YOUR MISSIONS?

Contact our HQ today

 tag.security@crayon.com

