RELIAQUEST®

Threat Landscape Report: Uncovering Critical Cyber Threats to Construction

Date: October 1, 2023 – September 30, 2024

Sector Overview

During the reporting period (October 1, 2023 to September 30, 2024), ransomware attacks on the construction sector rose by 41% from the previous year. This sector is particularly attractive to attackers due to its critical need to maintain operational continuity and avoid downtime, which cybercriminals exploit as leverage for ransom demands.

Organizations in the construction sector are particularly susceptible to phishing attacks, likely due to their extensive interactions with third parties and contractors, coupled with the high-pressure timelines of projects. These factors increase the likelihood of user interaction with phishing emails.

To effectively counter these risks, construction sector organizations should ensure security policies such as multifactor authentication (MFA) extend to third parties and contractors, invest in automated incident response strategies, and rigorously monitor cloud account permissions and suspicious recently created accounts.

Top MITRE ATT&CK Techniques

During the reporting period (October 1, 2023 to September 30, 2024), phishing emerged as the top initial access technique targeting our construction sector customers. Its enduring popularity among threat actors is likely explained by its high success rate and minimal resource investment. Within phishing, **spearphishing with links** (T1566.02) and **spearphishing with attachments** (T1566.01) dominated, accounting for 25% of the sector's alerts.

Phishing isn't just a construction sector problem—it's a leading threat across all industries. Spearphishing with links and attachments exploit end users through advanced social engineering methods, including quishing (QR code phishing) and AI-generated phishing webpages. These evolving tactics make it easier than ever to deceive users into revealing credentials or downloading malware.

The construction sector is especially vulnerable to phishing because of the substantial funds involved in projects and the extensive communication networks required for billing and project management. Attackers can seamlessly blend in with the multitude of third parties and contractors commonly used by construction companies. Employees are also more likely to interact with external emails, assuming they're from trusted partners, thereby increasing the chances of successful phishing attempts. The consequences of spearphishing can be severe, especially financially, with risks including stolen project finances, supplier payments, and payroll.

For the second consecutive year, **lateral movement** (TA0008) ranked second among MITRE tactics, making up 21% of the total alert volume in the sector. This tactic remains prevalent likely because it's usually a required step for threat actors to progress their attacks. At 16%, **internal spearphishing** (T1534) was the second most common MITRE technique against the construction sector. This technique involves attackers using compromised employee accounts to spearphish

other internal users, exploiting the trust that's often inherent in internal communications to boost engagement with phishing emails.

The time demands of construction projects can put pressure on users to quickly open and respond to emails—another factor attackers leverage to increase engagement. Successful internal spearphishing grants attackers access to other internal accounts. Based on past attacks, they likely use this access to infiltrate deeper into the network or acquire higher-level privileges, eventually deploying malware or pivoting further in the network. Once malware is deployed, systems can be taken offline through ransomware, or sensitive data such as employee personally identifiable information (PII) can be stolen.

As construction organizations expand globally, they need to adopt more technologies and network infrastructure[1]. To support this growth, many are embracing the cloud, driven particularly by the unique need to operate in remote and temporary locations that often have only temporary or no IT infrastructure. They also need scalable solutions to host diverse technologies, such as building management systems and machine software. Cloud deployment allows organizations to maintain mobile networks that can be accessed anywhere and quickly integrate new technologies. However, this shift introduces a new attack surface through **valid cloud accounts** (T1078.004), where threat actors exploit accounts used to manage or operate within the cloud for initial access, persistence, privilege escalation, or defense evasion. Once inside, it's realistically possible that they use the accounts to access sensitive cloud-stored data such as construction or engineering blueprints, which may contain proprietary information. This data is valuable and could be used by competitors to gain a market edge or by attackers to exploit the compromised organization.

MITRE ATT&CK ID	MITRE Technique	% of Incidents
T1566.002	Phishing: Spearphishing Link	19
T1534	Internal Spearphishing	16
T1566.01	Phishing: Spearphishing Attachment	7
T1078.004	Cloud Accounts	6
T1133	External Remote Services	6

Case Study: In April 2024, ReliaQuest responded to a phishing incident involving a customer in the construction sector. Our investigation revealed that the phishing email originated from a legitimate third-party company, but the email inbox of an employee at the third-party company had been compromised. The attacker used the compromised inbox to send a phishing email disguised as a response to a purchase order. The unsuspecting user clicked a link in the email, which directed them to a fake eFax page.

This page contained a message with a link to another domain that mirrored an Office 365 login page and hosted a credential harvester. This incident highlights the risks associated with third-party interactions and the consequences if they become compromised. Specifically, it demonstrates how threat actors take advantage of users' trust in established communication channels to achieve malicious objectives.

To remediate the incident, we worked with the customer to swiftly reset the compromised user's credentials, terminate their live sessions, purge all phishing emails, and block malicious artifacts. Construction sector organizations are particularly vulnerable to such attacks, as construction companies are known to interact with more third parties than any other sector, making vigilance and robust security operations measures essential.

GreyMatter Insights

ReliaQuest GreyMatter gathers security metrics across all industries, including the construction sector. A crucial metric is the mean time to contain (MTTC) threats, which measures the time from detecting a security incident to initiating a containment action. This statistic provides valuable insight into an organization's containment effectiveness. In the construction sector, organizations adopting GreyMatter's automation and AI and its Automated Response Playbooks achieve an average MTTC of four minutes. Although slightly higher than the all-sector average of three minutes, this is significantly better than those in the sector not using Automated Response Playbooks, who average four hours and 47 minutes.

It's difficult to pinpoint exactly why the construction sector experiences slower MTTC than other industries. One possible reason is the delay in remediation efforts caused by the need to track down endpoints across various remote and temporary job locations, which often have limited or no network access. This postpones remediation action until the defender and host can communicate, potentially taking hours or days. A method to directly address this challenge is by implementing Automated Response Playbooks, which swiftly apply containment measures as soon as a threat is detected, before a host goes offline from moving job sites or unstable connections.

Extended MTTC times drastically increase the risks associated with attacks for construction organizations as attackers have more time to compromise networks. Risks include damage to brand reputation from data leaks, operational downtime delaying projects and thereby causing financial losses, or malware deployment. Longer MTTC also adds stress to teams, potentially leading to burnout and employee turnover.

Case study: In September 2024, ReliaQuest responded to a malicious file alert for a construction sector customer. We discovered that the "SocGholish" (aka FAKEUPDATES) malware was delivered to a host through a compromised legitimate domain and drive-by downloads. The compromised website, related to building design guides, tricked the user into downloading a malicious file disguised as a browser update. This method highlights how attackers hijack weaker infrastructure to spread malware.

Once downloaded, the malware manipulated the Mark-of-the-Web (MotW) setting on a JavaScript (.js) file, allowing it to run without restrictions. MotW is a Windows feature that flags files downloaded from the web and limits their execution rights. The malware then used wscript to execute the JavaScript file and download a base64-encoded file, a tactic used to hide the file content from endpoint detection and response (EDR) tools and defenders.

We worked with the customer to block all malicious artifacts, isolate and re-image the host, rotate user credentials, and terminate live sessions. The tactics used in this incident are widely used among adversaries. Therefore, to better protect yourself from similar attacks, it's crucial to understand how this malware masquerades under legitimate domains, in this example from a construction company, and employs tactics like base64 encoding and MotW manipulation to avoid detection.

Findings from the Dark Web

Although chatter among threat actors about targeting the construction sector is limited on the dark web, construction-related data breaches still frequently appear. Initial access brokers (IABs) often sell account usernames and passwords on credential marketplaces and data-leak sites, exposing sensitive data. This contrasts with the health care and social assistance (HSA) sector, which has sparked heated debates on criminal forums due to ethical concerns and potential political fallout from attacking health care institutions. The construction sector doesn't have the same moral barriers or impacts, which is likely why there are fewer discussions on forums. The minimal forum activity also suggests that attacks on the sector are more opportunistic than targeted.

However, opportunistic attacks still pose a significant threat on the sector. The presence of construction company credentials and data on dark-web marketplaces and leak sites underscores the need for robust security measures. By strengthening authentication mechanisms, monitoring dark-web activity, enhancing data security, and preparing for incidents, construction companies can better protect themselves against these threats and mitigate potential impacts.

In September 2024, a user on the popular English-language forum BreachForums posted stolen data from a construction company (see Figure 1), hinting they might have even more or had only captured a portion of the organization's data. Not long after, another user provided instructions for using Zphisher, an open-source phishing tool, to further exploit the exposed data and create new attack opportunities against the company.

This incident showcases the severe repercussions of leaked company data, including the potential for resource development. It demonstrates how attackers readily share knowledge when convenient for them and how exposed data can inspire new attack methods. These tactics can lead to additional attacks on the organization, more data theft, ransomware deployment, or denial of service (DoS) attacks, all of which can significantly disrupt or halt operations.

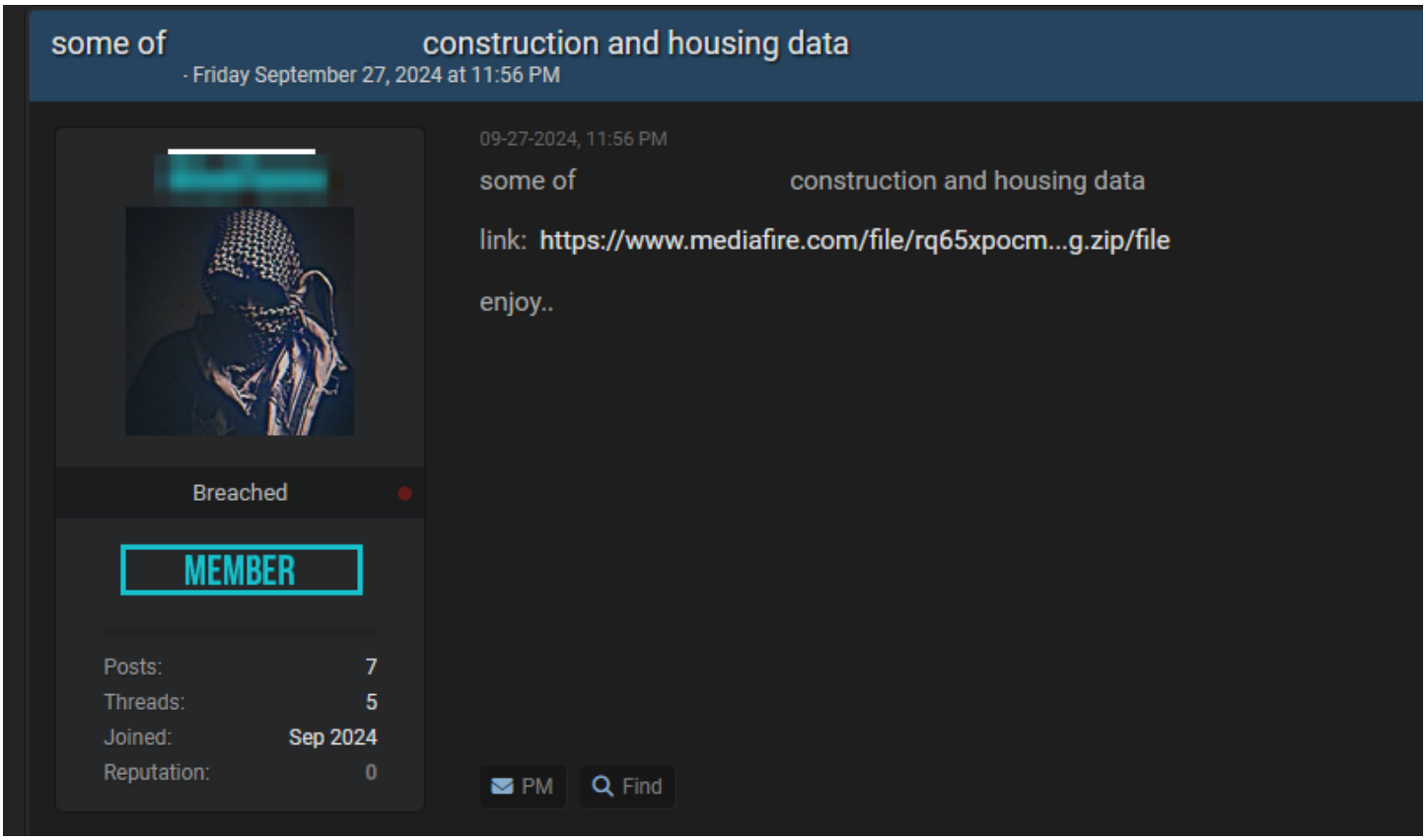

Figure 1: A user on BreachForums posting breached construction data for others to examine

Insights from GreyMatter Digital Risk Protection

Credential exposure is the top threat across all sectors, including construction. When a company's assets, like their domain or key personnel credentials, are identified in a credential sale on dark-web marketplaces, an alert is triggered to notify the escalation point of contact. In the current reporting period, credential exposure accounted for 75% of all GreyMatter Digital Risk Protection (DRP) alerts for the construction sector—a staggering 83% jump from the previous year. This spike in credential exposure alerts wasn't limited to construction; it was seen across the board, demonstrating the escalating threat of credential sales in every industry.

Construction companies have the highest rate of credential exposure alerts across all sectors, indicating they are the most targeted. This is possibly because credentials from construction companies are prized since they unlock access to sensitive data such as government contracts and building or infrastructure data. Another reason credential exposure is the top risk likely stems from the increased use of infostealers and the success of credential marketplaces on the dark web, such as Russian Market. From Q2 to Q3 of 2024 ReliaQuest observed a 58% increase in the number of information-stealing malware (infostealer) logs for sale on the dark web across all sectors. It's a significant increase from the 30.5% increase between Q3 and Q4 2023 that will likely continue to grow into 2025.

Sensitive data or credentials exposed on the dark web can have lasting impacts on construction sector organizations, giving criminals access to critical information. Cybercriminals use dark-web platforms to sell stolen credentials, publish

stolen data, or develop attack resources against specific software or organizations. Credentials are typically harvested using infostealers like “Lumma” and provide attackers with initial access to networks.

The credentials are usually sold as username or email and password pairs with additional information like the associated domain. This approach allows attackers to be more targeted in their purchasing of customer or employee credentials, so they will be more likely find the credentials they need to attack specific organizations. Published sensitive data can expose confidential customer, employee, or proprietary information, such as project bids and blueprints. These threats can lead to severe operational impacts, including malware attacks through purchased credentials, lost revenue, or brand damage from eroded trust among customers and partners.

Impersonating domain ranks as the second highest GreyMatter DRP risk, making up 15% of total sector alerts during the reporting period. **Impersonating sub-domain** follows in third at 8%, overtaking **marked document,** likely as a result of the rise in phishing attacks against construction companies. This trend reflects a consistent pattern with the previous year and other sectors, likely because these alerts flag domains or sub-domains that mimic an organization’s brand assets, usually to conduct phishing campaigns. This expansion of domain impersonation is driven by successful phishing campaigns in which threat actors impersonate construction-related third parties to manipulate the trust that employees in the construction sector have in their external partners. A successful compromise can damage an organization’s reputation, erode customer trust, and expose their employee credentials to threat actors, paving the way for further attacks.

GreyMatter DRP alerts empower organizations to continuously monitor for domain impersonation attempts so they can swiftly take remediation action, such as submitting takedown requests to domain registrars or internet service providers (ISPs). The alerts also offer active monitoring against credential sales, helping organizations significantly reduce the risk of damage from stolen employee and customer credentials by allowing for remediation before malicious users can exploit them.

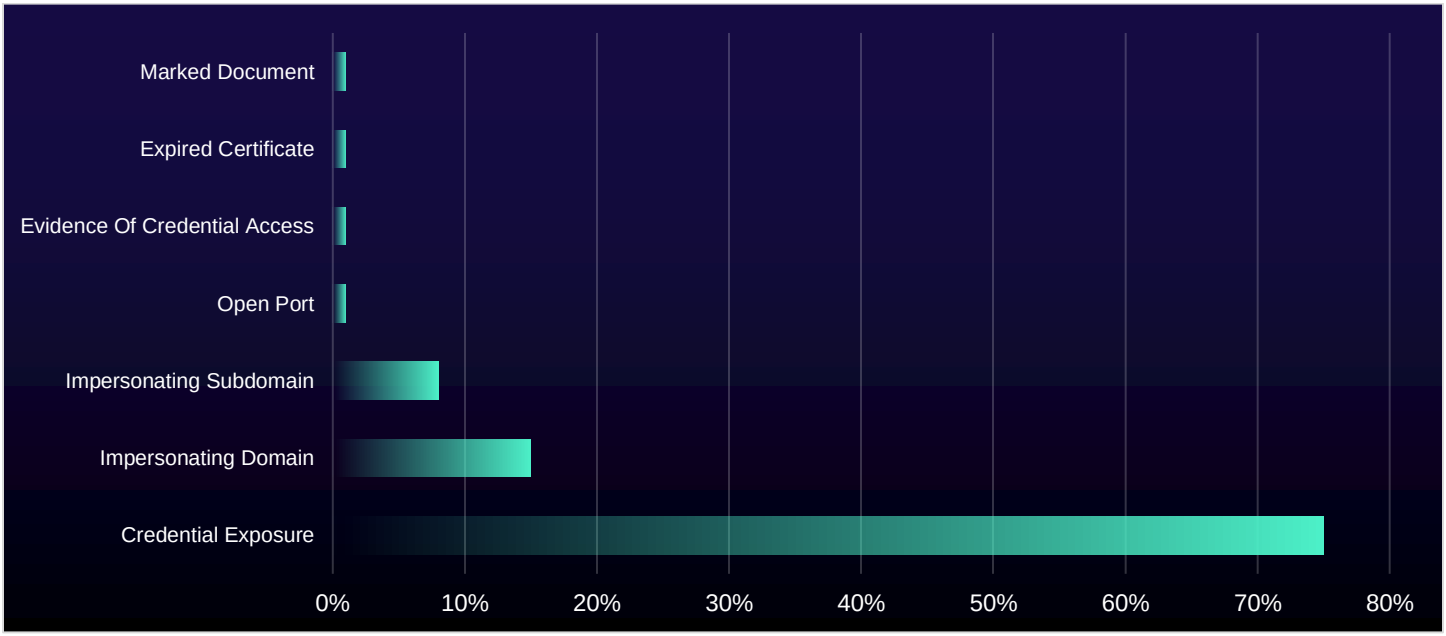

Figure 2: Percentage of GreyMatter DRP alerts for the construction sector

Ransomware Activity Targeting Construction Sector

Ransomware attacks against the construction sector grew during the reporting period, with 481 organizations named on ransomware data-leak sites, marking a 41% increase from the previous year. This rise is likely driven by opportunistic attacks on vulnerable companies rather than direct targeting of the construction sector. Construction companies probably find themselves in the line of fire more since they are often vulnerable due to the absence of stringent government regulations enforcing strong security controls and not investing enough in their security infrastructure. These factors leave them particularly exposed and easier targets compared to other sectors.

The shifting landscape of ransomware groups also likely contributes to the increase in attacks. Threat groups like “ALPHV” have disbanded, making way for the emergence of new ransomware-as-a-service (RaaS) groups such as “Meow” and allowing more established groups like “Play” to rise and take their places. These groups are seeking to make a name for themselves and expand their reach, ready to capitalize on the construction sector’s weaknesses and broaden their influence.

Appearing on a data-leak site can be devastating for an organization, compounding the damage of a ransomware attack. Posts quickly make news headlines when large organizations are listed, resulting in severe brand damage, exposure of proprietary assets, and potential legal troubles. To protect against ransomware threats, organizations should put in place strict data protection measures, such as implementing encryption, maintaining regular backups, and establishing robust access controls.

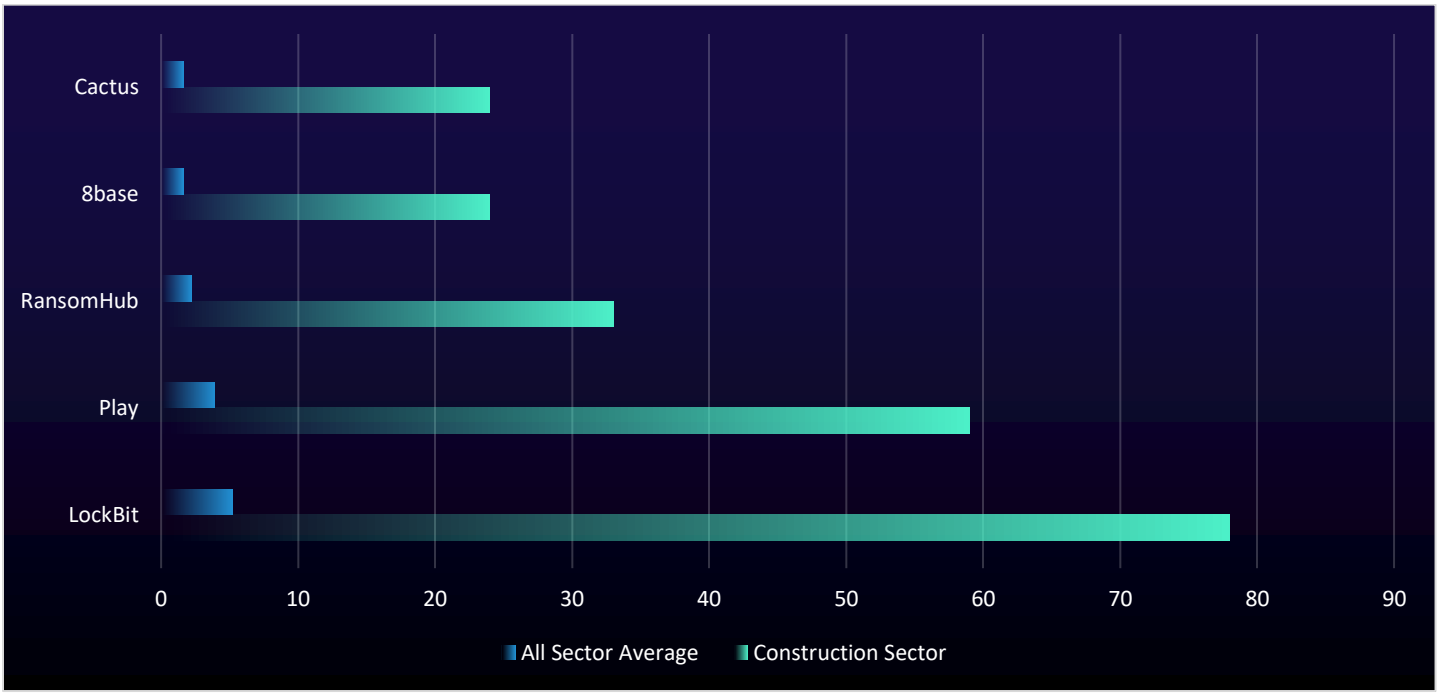

Figure 3: Construction companies named per ransomware group compared to all-sector average

Case Study: In October 2023, we responded to a malicious file alert impacting a customer in the construction sector. Our investigations revealed the execution of malicious commands and the deployment of “AsyncRAT,” a remote access trojan (RAT) that provides threat actors with remote desktop, file explorer, keylogging, and process manager functionalities.

The attacker used the Windows Script Host (wscript) executable to execute a malicious Windows Script File (.wsf). Although data retention limitations prevented us from pinpointing the initial download method, these files are typically delivered via phishing or search engine optimization (SEO) poisoning. The attacker also used the PowerShell cmdlet Invoke-Expression to download two text (.txt) files from a command-and-control (C2) server. Finally, the attacker attempted to evade defenses by using the Windows Device Enroller executable to disable Windows Defender on the compromised host.

To contain and mitigate the attack, we recommended the customer isolate and re-image the infected host, reset user credentials, terminate any active sessions, and block all malicious artifacts. Ransomware attacks are a growing threat for construction companies and this incident provides insight into the early stages of a ransomware attack. This enables organizations to better prepare and bolster their defenses from similar threats.

Key Threat: Play

Also known as “PlayCrypt,” Play is a financially driven ransomware group that uses double extortion tactics—encrypting data to take systems offline and exfiltrating sensitive information—to pressure organizations into promptly paying ransoms.

Ransomware remains the top threat to the constructor sector due to its high success rate against organizations in the sector. While Play doesn’t focus its malicious activities on any single industry exclusively, it still targeted 59 construction companies out of its 362 total targets during the reporting period. This number is only surpassed by the ransomware group “LockBit.” However, LockBit’s operations have since slowed following infrastructure disruptions caused by the FBI and other agencies. This decline has enabled Play to broaden its reach and become the biggest threat to construction companies, as demonstrated by the increasing number of organizations it has compromised.

Play employs a sophisticated array of techniques in its attacks. Notably, it uses popular tools like Cobalt Strike for post-compromise C2 activities and “SystemBC,” a remote access trojan (RAT), for gaining access and maintaining persistence on compromised hosts. To remain undetected within a network, Play uses Living off the Land binaries (LOLBins), an advanced tactic that exploits native Windows or other operating system processes to evade detection, rather than deploying malware. Play’s mastery of diverse, complex tactics, combined with its technical ability to build custom tools for exploitation and exploit new vulnerabilities, makes Play a formidable adversary for construction organizations.

One reason Play targets the construction sector is the sensitive data these organizations hold. For example, two construction companies, the Crain Group and Clabots, had their data leaked online by Play within the last year. This data included private identification information, legal documents, and tax records. To mitigate this threat and safeguard critical data, organizations should implement data loss prevention (DLP) software to detect and block unauthorized access and exfiltration of intellectual property, such as architectural or engineering designs, and other data that could disrupt operations. Group Policy Objects (GPOs) should be used to globally disable or restrict remote access software frequently exploited by Play, such as Remote Desktop Protocol (RDP) and SystemBC, as well as lateral movement tools like PsExec.

To effectively defend against Play’s tactics and techniques, we recommend ReliaQuest customers prioritize rapid detection and containment by deploying the following GreyMatter detection rules. For the quickest remediation, automated incident response should be enabled by deploying Automated Response Playbooks to automatically contain threats upon detection. This improves MTTC and significantly reduces the risk of a full-blown attack. Alternatively, set GreyMatter Response Playbooks to “RQ Approved” to allow our analyst team to handle remediation on your behalf, further accelerating the response process.

Detection Rule	MITRE Technique	Summary
RQ – Cobalt Strike Named Pipe Created	T1572 – Protocol Tunnelling T1071 – Application Layer Protocol T1559 – Inter-Process Communication T1570 – Lateral Tool Transfer	This rule targets a specific feature of the Cobalt Strike C2 framework, which Play has used in previous campaigns. The named pipe feature allows attackers to establish an encrypted communication channel between two processes on the same system. This rule detects these named pipes by identifying signatures that are characteristic of Cobalt Strike.
RQ – Remote Access Software Service Installed – Critical Host	T1070.009 – Clear Persistence T1219 – Remote Access Software T1543.003 – Windows Service T1021.005 – VNC	To connect to a compromised host, Play deploys remote access tools like “SystemBC.” This rule detects when a remote access tool is running on a critical host.
RQ – PsExec Pivoting	T1021.002 – SMB/Windows Admin Shares T1569.002 – Service Execution	Play uses PsExec to connect to the network share of an internal host and execute commands on it. This rule detects when PsExec is executing on a host.

Isolate Host: Once a host is compromised and threat actor activity has been detected, the host should be isolated from the network. This Response Playbook prevents worms like ransomware and other malware from communicating with C2 servers and stops them from spreading to additional hosts within the environment.

Block Hash: Malicious files like ransomware have unique identifying hashes that verify the file's contents. These hashes can be added to security tools like EDR tools and intrusion prevention systems (IPSs) through Automated Response Playbooks to prevent them from executing on hosts within the environment.

Terminate Live Sessions and Reset Password: When a user's account is compromised and an attacker has access to it, they often exploit the access to advance their attack along the kill chain. Their objectives typically include compromising additional accounts, moving laterally to other hosts, or deploying malware. By terminating live sessions, all current sessions of the compromised account are immediately logged out. When combined with a password reset in an Automated Response Playbook, this action forces the attacker out of the account and prevents them from regaining access.

Cyber Threat Forecast for Construction Sector

Phishing and Social Engineering: Phishing attacks on the construction industry will likely continue to increase as a result of the sector's heavy reliance on third parties and contractors. These external players often lack essential security training and acceptable use policies, increasing their—and consequently the construction companies'—vulnerability to phishing attacks. Adversaries often employ a two-pronged approach, using social engineering tactics to exploit the urgency of tight project deadlines, tricking users into hastily interacting with phishing emails.

To combat these threats, organizations should enforce the principle of least privilege (PoLP) for all third parties and contractors; and extend security controls like multifactor authentication (MFA) policies and phishing training to everyone involved, not just internal employees. For mission-critical tasks, especially those involving banking and sensitive information, organizations should implement strict standard operating procedures (SOPs), including additional contact methods outside of email to verify if emails are legitimate or phishing.

Cloud Exploitation: Threat actors will highly likely step up their targeting of cloud services in the mid-term (three months to one year). We make this assessment with high confidence, because not only was attacking cloud accounts among the top five MITRE techniques in customer alerts for this sector, but global spending on public cloud services is projected to double by 2028[2]. Construction companies are particularly drawn to cloud solutions due to their need to operate in remote or temporary locations and support a wide range of technologies, such as sensors, drones, and wearable tech. However, defending the cloud can be challenging, given the limited tools and expertise available, which attackers exploit to evade detection and maintain access.

To counter these threats, organizations should enforce rigorous auditing of cloud accounts and resources; pay close attention to cloud permission levels that could grant extensive access, like global administrators; and also monitor for newly created privileged accounts that haven't been authorized.

Infostealers: Given the increasing volume of infostealer logs for sale on criminal marketplaces, as highlighted by GreyMatter DRP data, it's highly probable that attacks targeting the construction sector will rise in the mid-term (three months to one year). Infostealer malware seeks to compromise user credentials, which are then sold on dark-web forums. Armed with these credentials, buyers can gain access into systems. This access will likely be used to target sensitive construction sector information like engineering blueprints and data within building information modeling systems (BIMs). Attackers may also deploy additional malware within the environment to disrupt operations and inflict extensive damage.

To defend against infostealers, organizations should implement a digital risk protection (DRP) strategy to continuously monitor for exposed credentials. These solutions notify organizations when credentials have been exposed on the dark web, allowing for swift remediation actions such as implementing password resets. For an extra layer of security, organizations should also enforce MFA for all user accounts to help prevent account compromises even if credentials have been purchased by an attacker.

Conclusion

In the upcoming year, we expect the uptick of attacks targeting the construction sector to continue, including ransomware, phishing, and cloud-based attacks. This projection is guided by the rise in malicious activity and success of ransomware groups during the reporting period. Moreover, the construction sector faces unique challenges that leave companies vulnerable, making them attractive targets for threat actors. This underscores the critical need for organizations in the construction sector to take comprehensive security measures to harden their defenses and mitigate associated threats.

Organizations must extend robust security protocols to third parties and contractors to ensure these external partners don't become weak links in their security operations. Investing in proper employee education is also crucial to foster vigilance against phishing attempts, and a comprehensive DRP strategy and tailored defensive solutions should also be implemented to proactively counter ransomware and credential abuse stemming from dark web sales.

The ReliaQuest GreyMatter security operations platform enables organizations to efficiently and accurately detect malicious activity across multiple endpoints and security tools. With GreyMatter Hunt packages, companies can proactively identify potential threats, while Automated Response Playbooks provide rapid threat containment upon detection. In addition, by integrating DRP and leveraging threat intelligence, construction companies can preemptively mitigate risks before they escalate into threats, thereby significantly enhancing their overall security posture.

---

[1]hxxps://www.rics[.]org/content/dam/ricsglobal/documents/research/Digitalisation%20in%20construction%202023_final.pdf
[2]hxxps://www.idc[.]com/getdoc.jsp?containerId=prUS52460024#:~:text=NEEDHAM%2C%20Mass.%2C%20July%2029,Public%20Cloud%20Services%20Spending%20Guide.