Understanding Ransomware in AEC

Introduction

Ransomware has become the #1 threat in cybersecurity and one of the top 10 threats to humanity. 65% of enterprises with 100-5000 people have experienced at least one successful ransomware attack in the past year. In 2021, the average payment reported was $812,360, an increase of almost five times from $170,000 in 2020. Most companies pay to recover. The total amount of damage caused by ransomware is more than doubling each year, averaging $1.4M in 2021. AEC firms are twice as likely to be hit by ransomware than other corporations.

In this document, we discuss the findings as to why AEC companies are twice as likely to be hit by ransomware, what actually transpires when one gets hit by ransomware, and what AEC firms can do to address this issue. We thank Eric Quinn, CIO of C&S Companies, and Andy Knauf, CIO of Mead and Hunt for their detailed insights into AEC firms, along with several Nubeva IR partners in discussing the detailed process of going through a ransomware event.

Mead&Hunt

C&S COMPANIES®

Azure

Ransomware 2x More Likely In AEC

There are several reasons why AEC companies are twice as likely to be hit by ransomware than typical enterprises.

Distributed Apps & Workforce

AEC firms rely on geographically distributed design and development teams to gain an edge in providing better customer response while facilitating a better talent pool. "It's not unusual for an AEC firm to grow from 600-800 people and 8 sites while another shrunk from 1300-1200 people and shutdown 5 sites in the same year," said Knauf of Mead & Hunt.

To grow and shrink at this rate, AEC firms are constantly hiring and letting go of contractors, buying and selling businesses, and having to integrate different systems together. All the while, workers are moving between competitive firms.

One of the companies we spoke with was hit by ransomware 3 times. They noticed that each attack occurred shortly after releasing contractors from projects. The company could never correlate the ransomware events to the contractors, but one doesn't need to be a rocket scientist to know that they had to be related, either as true insider malicious behavior or simply as an outcome of human errors and change.

Further, whereas enterprises across other verticals heavily use contractors, they typically have more simple, processed-based, and often centralized web applications that are easy to use. AEC firms use complex and highly-distributed CAD and BIM applications such as AutoCAD and Revit. These Microsoft Windows apps provide a rich and flexible experience to meet their customers' exact needs. Any design change on an airport runway or a simple wall change in a building requires precise components to be matched for regulatory purposes and better visualizations. Apps like Revit open the same set of files on a file share across multiple geographical locations, making it behave very similar to how a ransomware/malware would act in its spread.

In a MITRE 2022 report, the #1 technology to prevent malware is Endpoint Detection and Response systems (EDRs.) Most have a prevention rate well under 89%, with Microsoft security running under 85%.

		Detection Rate	Prevention Rate	Total Rating
1	SentinelOne	99.08%	89.91%	94.50%
2	cybereason	100%	87.16%	93.58%
3	paloalto	98.17%	88.99%	93.58%
4	Cynet	98.17%	88.07%	93.12%
5	CROWDSTRIKE	96.33%	84.40%	90.37%
6	Microsoft	89.91%	85.32%	87.61%
7	TREND MICRO	96.33%	71.56%	83.94%
8	Malwarebytes	92.22%	67.89%	80.06%
9	McAfee	98.17%	59.63%	78.90%
10	FORTINET	96.67%	60.55%	78.61%
11	CYLANCE	81.65%	75.23%	78.44%
12	AhnLab	92.22%	61.47%	76.85%
13	CISCO	82.57%	67.89%	75.23%
14	Check Point	94.50%	55.96%	75.23%
15	FIREEYE	81.65%	55.05%	68.35%

		Detection Rate	Prevention Rate	Total Rating
16	vmware Carbon Black	82.57%	50.46%	66.51%
17	Symantec	84.40%	47.71%	66.06%
18	SOPHOS	80.73%	44.95%	62.84%
19	eset	83.33%	33.94%	58.64%
20	deep instinct	70.00%	46.79%	58.39%
21	CYCRAFT	70.64%	39.45%	55.05%
22	Bitdefender	97.25%	0%	48.62%
23	elastic	89.91%	0%	44.95%
24	Uptycs	84.40%	3.67%	44.04%
25	Fidelis	86.24%	0%	43.12%
26	REAQTA	78.89%	0%	39.44%
27	F-Secure	76.15%	0%	38.07%
28		75.56%	0%	37.78%
29	Qualys.	73.33%	0%	36.67%
30	RAPID7	56.88%	0%	28.44%

These systems rely heavily on behavior analysis to achieve those results. But in AEC, the EDR and security systems' outcomes are much lower as behavior analysis is exceptionally difficult to distinguish between a proper file lock in Revit across multiple geographies that massively change the contents of several files simultaneously, versus the behavior of ransomware.

Frequent M&A Activity Creates More Exposure

As discussed in the previous section, AEC firms are highly distributed for numerous reasons specific to their industry, which results in parts or whole companies frequently under M&A or contracting. One of the top targets for bad actors is companies engaging in M&A. In March 2022, the Wall Street Journal article "Ransomware Attackers Begin to Eye Mid Market Acquisition Targets" validated what the cyber security industry has been observing for months as a growing trend. But unlike hedge funds and banks with significant cybersecurity budgets, AEC firms are not financed well enough to adequately protect against the levels and frequency of cyberattacks.

In one example, an AEC company of 900 employees increased its headcount by 400 in three years through numerous acquisitions. 100% of those acquired had users with laptops and servers with administrator rights. Most, if not all, were running Windows 10 that were several months behind in patches. As discussed in the previous section, keeping all Windows systems fully up to date provides only an 85% breach protection.

Another AEC firm with 800 people shrunk and sold off one-quarter of its workforce. They were running an EDR with full IR protection. Yet not a single one of the acquiring companies used the same EDR.

What Actually Happens In a Ransomware Event

Up to 72 hours before a ransomware event is typically when a bad actor penetrates and erases all its footprints. This includes cleaning all of the logs of access and movement, disabling and removing snapshots and backups, and starting the distribution of ransomware binaries across the entire enterprise. It observes and learns normal patterns of behavior and operations to execute within the target environment undetected and gain leverage. For example, a minor update to a Revit BIM file opened across 8 geographies in a file share will create a domino effect to update all sites and all affected files everywhere. A ransomware gang will learn and mimic this behavior to spread across an organization without detection. Unlike a Google docs change, that for the most part, involves a change between the client and Google's servers, CAD and BIM changes occur directly on a Windows file share, precisely what malware preys upon.

A major ransomware family such as Conti or Lockbit (which combined contributed to over 50% of attacks over the last year) typically has thousands of affiliates around the world. Each affiliate has a role. One may offer $5,000 in bitcoin to gain credentials into an organization, no questions asked. This simple incentive is said to be the root cause of thousands of attacks globally. All it takes is one disgruntled or naive employee or

contractor to click a link, and "voila" a back door is opened. Another might be an expert in using such credentials to get into an org while staying hidden. Another set of affiliates may create different versions of the ransomware, so each incident generates a new signature, thus avoiding traditional signature-based cybersecurity products. And finally, ransomware groups provide impressive customer service with 24/7 support on discord (fully anonymous) servers to support payment questions and data recovery. Together it has become a frightening, multi-level ecosystem and high-growth crime industry.

Prior to detonation, ransomware gangs surveil the networks, computers, and data sets. They analyze business operations and operating models to identify the maximum potential for business interruptions to maximize the ransom. Finally, they determine how to circumvent immutable storage, cloud snapshots, cloud drive, and backup systems. Once ransomware detonates, it starts massively expanding across an org using very sophisticated multi-threaded techniques and can encrypt files at multi-gigabit rates. Multi-billion dollar firms with complex EDR and AI-based cybersecurity solutions have been known to be taken down in a matter of minutes.

So You've Been Ransomed, Now What?

In one of the companies ransomed, an 80-person AEC company, composed primarily of designers, was in the process of being purchased by another form of 1300 people. Once they were ransomed, they went radio silent with their potential acquirer, fearing that the deal or the price of the M&A deal would be negatively affected. Their ransom was for

$200,000, and restoring from backup would take them 22 days, and cloud snapshots would take more than 7 days to fully correlate all the data on laptops and servers together to bring the business up again. So the company's stakeholders agreed to pay the ransom. They contacted their cyber insurance carrier, who brought in lawyers and an IR firm to negotiate to pay off the ransom.

The law firm advised the company that the US government had recently enacted rules prohibiting the payment to companies affiliated with specific countries. The liability of this issue was difficult to assess given that even if they were willing to take a chance, their acquirer may not. Another firm was brought in to make the payment, and ensure the payment was not to a group blacklisted by the government. Once payment was made, the IR firm interacted with the bad actors over discord servers to gain access to the decryption key and restore their data. Support from the bad actors over the discord servers was excellent and reliable. It took 3 days to decide to pay the bad actors, fully restore, and bring the business back to normal. The larger company successfully acquired the 80-person company, and all is well.

This is one of the many reasons why the vast majority of the people targeted by ransomware pay. The options are limited, and the bad actors have built an extremely reliable support system to fully restore businesses back to normal once they pay.

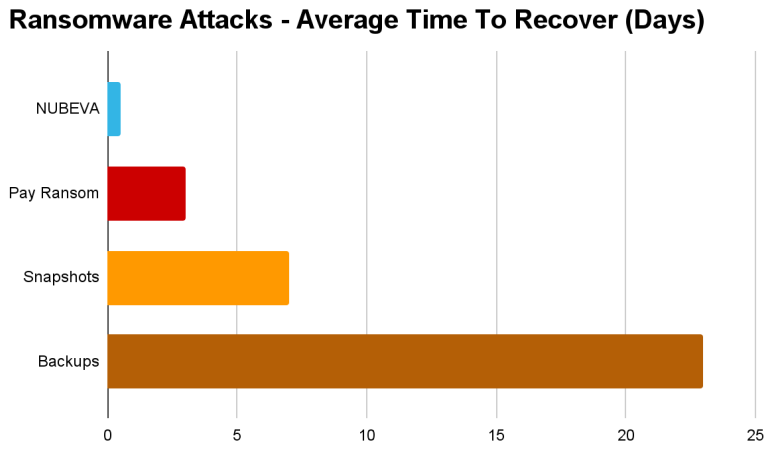
How Nubeva Would Have Helped

The premise of Nubeva is simple: It's not a matter of "IF" but of "WHEN" and "HOW BAD". When it happens, Nubeva will recover data and restore it faster and easier than backup systems and will minimize costs, downtime, and business damages.

Whereas the entire cybersecurity industry is trying to detect and block over 30,000 variants from 100+ ransomware gangs and families, Nubeva detects malicious file encryption using the less than 10 stable, viable methods used over the past 40 years. Our ransomware solution reliably detects their attack and intercepts copies of the encryption keys they use to lock your files. Then, when the attackers are gone, with copies of the keys in hand, Nubeva enables fast, easy, and efficient decryption of your files to reverse the attack… without paying the ransom.

Nubeva Value

After a successful ransomware attack, restore your plans, drawings, proposals, deliverables, and other mission-critical data faster, easier, and at a lower cost.



Looking back at our previous example of the 80 person AEC firm, if Nubeva had been installed the attackers would still have breached their network, they still would have installed ransomware on all laptops, desktops, and servers, and they still would have detonated the ransomware thus encrypting everything followed by a ransomware note left on each screen, and the firm would have still called their Cyber Insurance carrier. But instead of bringing in lawyers to pay the ransom, Nubeva would have provided the decryption keys and support to fully decrypt all the files in about the same time it took to encrypt them in the first place. With Nubeva, all of the data would be back in hours, without paying a ransom and without working with criminals. Better still, the majority of the Nubeva solution costs would be paid for by emergency funds and insurance coverage.

"I believe what Nubeva is doing is a game-changer. For us, it was a no-brainer decision. It was easy to install, trivial to run, and extremely affordable. I sleep better knowing we have it."

Eric Quinn, CIO of C&S Companies

To learn more about how Nubeva can help you: www.nubeva.com

To request an overview or demonstration: info@nubeva.com or 844.538.4638