Allied Universal Breached by Maze Ransomware, Stolen Data Leaked

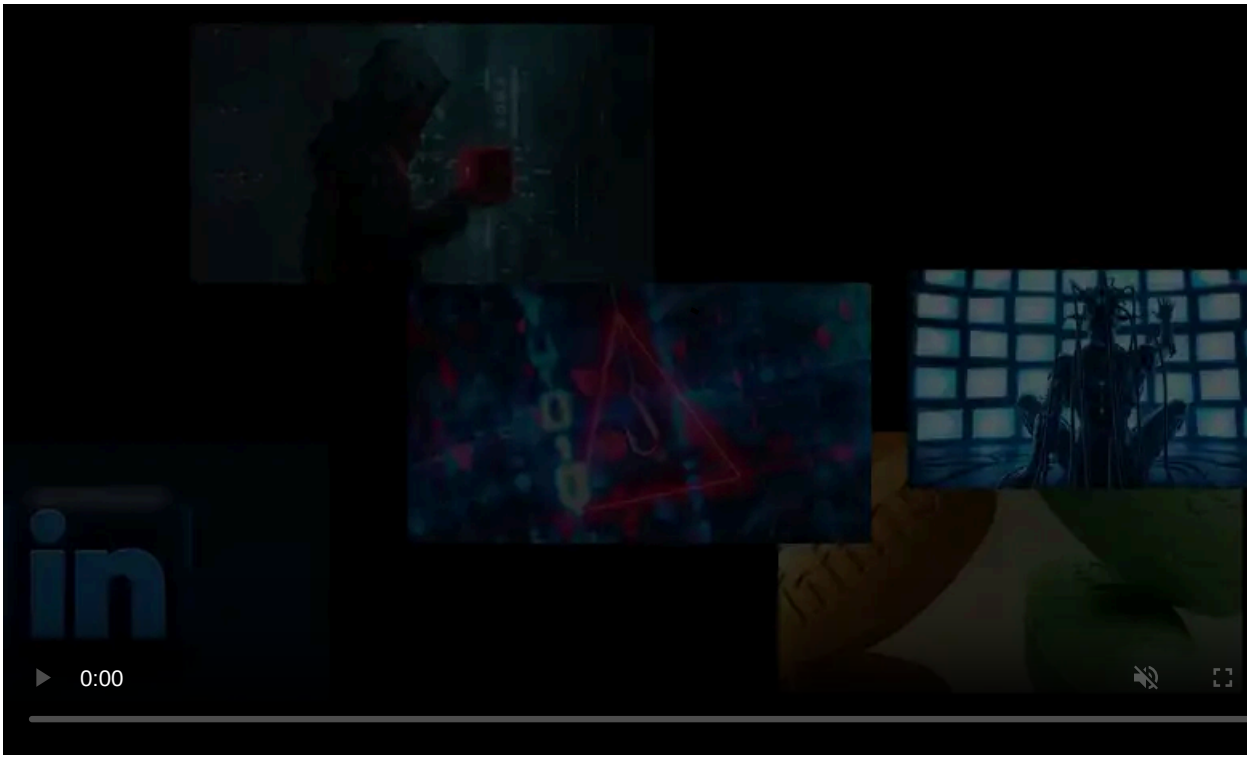
By Lawrence Abrams

Published: 2019-11-22 · Archived: 2026-04-05 16:34:16 UTC

After a deadline was missed for receiving a ransom payment, the group behind Maze Ransomware has published almost 700 MB worth of data and files stolen from security staffing firm Allied Universal. We are told this is only 10% of the total files stolen and the rest will be released if a payment is not made.

This is an unfortunate story and one that BleepingComputer does not enjoy telling, but with Maze's actions it is important to be told.

With this escalated attack, victims now need to not only be concerned about recovering their encrypted files, but what would happen if their stolen unencrypted files were leaked to the public.


0:00

Maze Ransomware contacts BleepingComputer

Maze is a ransomware infection that been operating for some time, but has become increasingly more active since May 2019. The affiliates of Maze are also becoming more known, with ProofPoint identifying one as TA2101 after seeing them conduct numerous malspam campaigns that impersonate government agencies.

Last Friday at 6:35 PM EST as I was finishing for the day, I received an email from a known email address utilized by the Maze Ransomware.

This email was signed from the 'Maze Crew' and was about how they breached a large security staffing company named Allied Universal, who employs approximately 200,000 people and has revenues of over $7 billion USD.

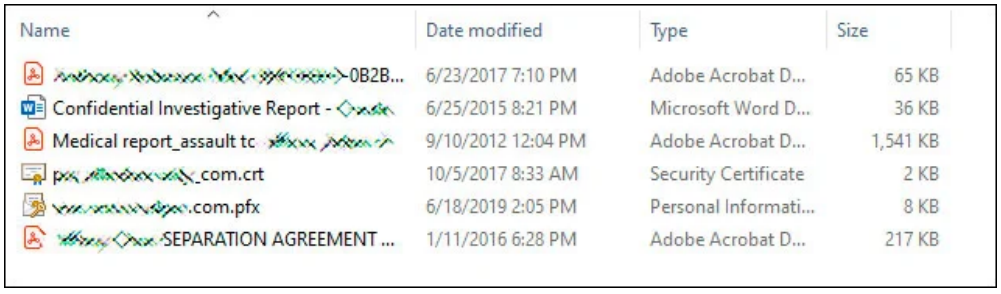
"I am writing to you because we have breached Allied Universal security firm (aus.com), downloaded data and executed Maze ransomware in their network.

They were asked to pay ransom in order to get decryptor and be safe from data leakage, we have also told them that we would write to you about this situation if they dont pay us, because it is a shame for the security firm to get breached and ransomwared.

We gave them time to think until this day, but it seems they abandoned payment process.

I uploaded some files from their network as the data breach proofs. If they dont begin sending requested money until next Friday we will begin releasing on public everything that we have downloaded from their network before running Maze."

Included in this email was a small sample of files that were allegedly stolen from Allied Universal. After being reviewed by BleepingComputer, these appeared to be legitimate files stolen from the company.



Name	Date modified	Type	Size
[redacted]-0B2B...	6/23/2017 7:10 PM	Adobe Acrobat D...	65 KB
Confidential Investigative Report - [redacted]	6/25/2015 8:21 PM	Microsoft Word D...	36 KB
Medical report_assault tc [redacted]	9/10/2012 12:04 PM	Adobe Acrobat D...	1,541 KB
[redacted]_com.crt	10/5/2017 8:33 AM	Security Certificate	2 KB
[redacted].com.pfx	6/18/2019 2:05 PM	Personal Informati...	8 KB
[redacted] SEPARATION AGREEMENT ...	1/11/2016 6:28 PM	Adobe Acrobat D...	217 KB

Sample of stolen Allied Universal files

In further conversations, the Maze actors told us that they encrypted 'a lot' of computers and are demanding 300 bitcoins, or approximately $2.3 million USD, to decrypt the entire network.

They went on to tell us that before they encrypt any computer, they always exfiltrate, or steal, a victim's files so it can be used as further leverage to have the victim pay the ransom.

When I asked what assurances the victims have that Maze will actually delete the files, we were told they were not interested in their data, just their money.

"It is just a logic. If we disclose it who will believe us? It is not in our interest, it will be silly to disclose as we gain nothing from it. We also delete data because it is not really interesting. We are neither espionage group nor any other type of APT, the data is not interesting for us."

When we contacted Allied Universal to not only get a statement, but to also warn them about the Maze crew's threats, we were told the situation was under investigation.

"Allied Universal is aware of a situation that may involve unauthorized access to our systems. We take any situation of this nature very seriously. This incident is being thoroughly investigated by Allied Universal IT experts who have taken immediate and appropriate actions to reinforce existing security measures and to mitigate any potential impact. We also have

engaged outside cybersecurity experts to re-verify our system's security. Keeping our company data safe and that of our customers and employees is of paramount importance," Allied Universal told BleepingComputer in a statement.

Further attempts to contact Allied were met with them stating that they "will not be providing any additional comment at this time."

Over the next couple of days, Maze told us that they continue to have access to the company's servers and shared a list of file names associated with TLS and email signing certificates.

They further warned that if Allied Universal did not pay, the Maze actors would conduct a spam campaign using Allied's domain name and email certificates.

"Ask them a question: would they like if next Monday TA2101 impersonate Allied Universal in a spam campaign using the next certs? Saving pfx's plaintext password in pw.txt is so secure for a security company. LMAO. I think you should write amazing article about this. Name it: "HOWTO: The easiest way for a security company to be f**ked up"

After a lack of negotiation occurring between Maze and Allied Universal, the Maze actors more pointedly indicated that BleepingComputer should publish a story about what was happening.

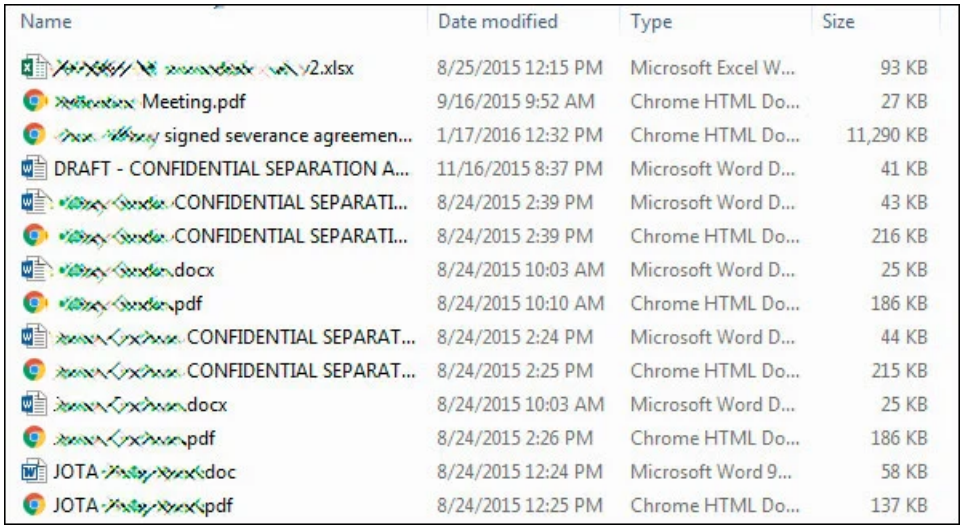
BleepingComputer did not feel comfortable being used as leverage in their negotiations. Instead we decided to wait until either Allied Universal paid the ransom, the company issued a public statement, or stolen files were leaked

Maze releases some of the Allied Universal files

Knowing that tomorrow was Maze's deadline, we were surprised tonight when they posted in our forums a description of the breach and a link to almost 700 MB of leaked files.

"We have already morning of Friday. Yes, it is friday in asia. Forgot to mention that deadline is a friday by our local time, and not US."

This link was for a 7-zip archive containing files related to termination agreements, contracts, medical records, server directory listings, encryption certificates, and exported lists of users from their active directory servers.

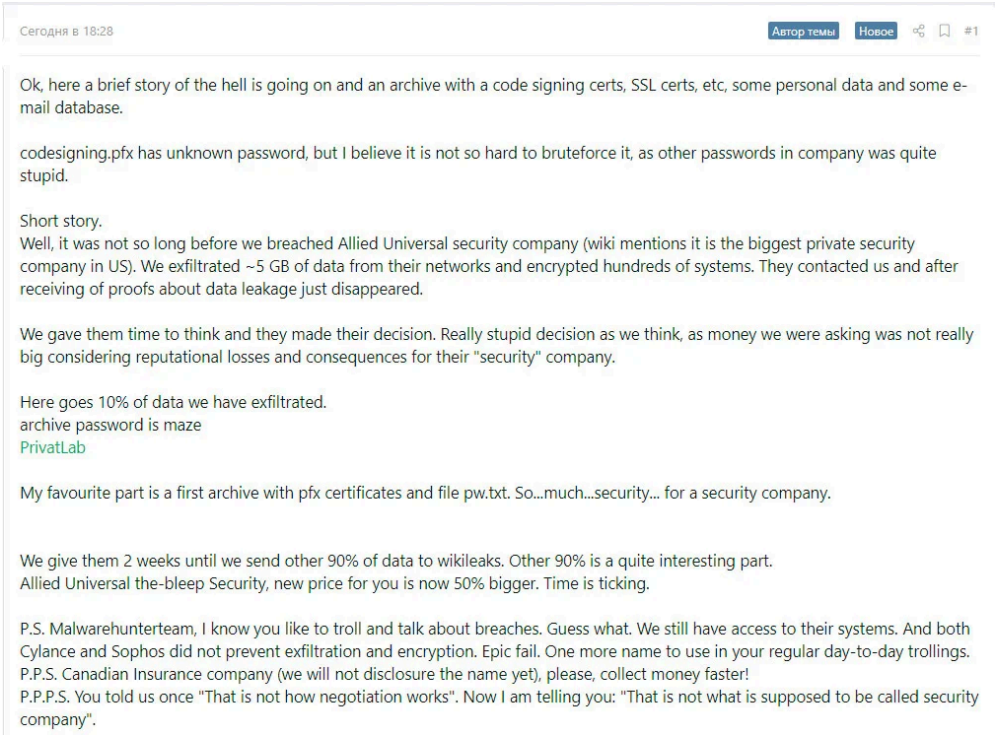


Name	Date modified	Type	Size
[redacted]v2.xlsx	8/25/2015 12:15 PM	Microsoft Excel W...	93 KB
[redacted] Meeting.pdf	9/16/2015 9:52 AM	Chrome HTML Do...	27 KB
[redacted] signed severance agreemen...	1/17/2016 12:32 PM	Chrome HTML Do...	11,290 KB
DRAFT - CONFIDENTIAL SEPARATION A...	11/16/2015 8:37 PM	Microsoft Word D...	41 KB
[redacted] CONFIDENTIAL SEPARATI...	8/24/2015 2:39 PM	Microsoft Word D...	43 KB
[redacted] CONFIDENTIAL SEPARATI...	8/24/2015 2:39 PM	Chrome HTML Do...	216 KB
[redacted].docx	8/24/2015 10:03 AM	Microsoft Word D...	25 KB
[redacted].pdf	8/24/2015 10:10 AM	Chrome HTML Do...	186 KB
[redacted] CONFIDENTIAL SEPARAT...	8/24/2015 2:24 PM	Microsoft Word D...	44 KB
[redacted] CONFIDENTIAL SEPARAT...	8/24/2015 2:25 PM	Chrome HTML Do...	215 KB
[redacted].docx	8/24/2015 10:03 AM	Microsoft Word D...	25 KB
[redacted].pdf	8/24/2015 2:26 PM	Chrome HTML Do...	186 KB
JOTA [redacted].doc	8/24/2015 12:24 PM	Microsoft Word 9...	58 KB
JOTA [redacted].pdf	8/24/2015 12:25 PM	Chrome HTML Do...	137 KB

More leaked files

As I was not going to allow BleepingComputer to be used to distribute stolen data, I deleted the post from our forums.

In a later email to us they shared a link to a post on a Russian hacker and malware forum that once again describes the breach and also contains a link to the leaked data. They also stated that they will distribute the other 90% of the leaked data to WikiLeaks if an increased ransom of $3.8 million dollars is not paid.



Сегодня в 18:28 Автор темы Новое #1

Ok, here a brief story of the hell is going on and an archive with a code signing certs, SSL certs, etc, some personal data and some e-mail database.

codesigning.pfx has unknown password, but I believe it is not so hard to bruteforce it, as other passwords in company was quite stupid.

Short story.
Well, it was not so long before we breached Allied Universal security company (wiki mentions it is the biggest private security company in US). We exfiltrated ~5 GB of data from their networks and encrypted hundreds of systems. They contacted us and after receiving of proofs about data leakage just disappeared.

We gave them time to think and they made their decision. Really stupid decision as we think, as money we were asking was not really big considering reputational losses and consequences for their "security" company.

Here goes 10% of data we have exfiltrated.
archive password is maze
PrivatLab

My favourite part is a first archive with pfx certificates and file pw.txt. So...much...security... for a security company.

We give them 2 weeks until we send other 90% of data to wikileaks. Other 90% is a quite interesting part.
Allied Universal the-bleep Security, new price for you is now 50% bigger. Time is ticking.

P.S. Malwarehunterteam, I know you like to troll and talk about breaches. Guess what. We still have access to their systems. And both Cylance and Sophos did not prevent exfiltration and encryption. Epic fail. One more name to use in your regular day-to-day trollings.
P.P.S. Canadian Insurance company (we will not disclosure the name yet), please, collect money faster!
P.P.P.S. You told us once "That is not how negotiation works". Now I am telling you: "That is not what is supposed to be called security company".

Post on Russian hacker and malware forum

This increased amount is highly unlikely, as Maze told us that in their negotiations with Allied Universal, the company said they would pay no more than $50,000 USD.

Now that the data and breach had been publicly disclosed by the Maze actors, we contacted law enforcement, once again attempted to contact Allied without a response, and decided to write this article.

What does this mean going forward?

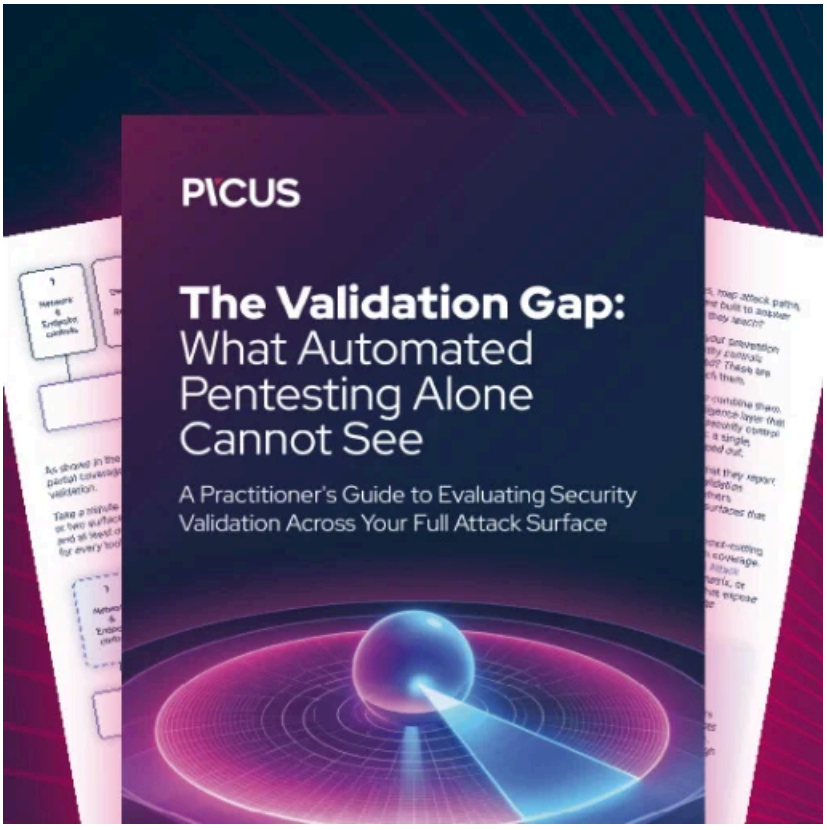
While many ransomware developers have threatened to release data if a ransom was not paid, this is the first time we know of that it has actually happened and in such as a visible manner.

With threat actors escalating their attacks to public disclosure of confidential and sensitive files, victims need to weigh the cost of ransomware payments versus the potential costs of sensitive employee and business information or confidential trade secrets being released to the public.

Furthermore, with ransomware actors actively searching through files on a victim's machines in order to further extort their victims, in many cases these attacks should now be considered data breaches.

This leads to an escalated cost of dealing with breach notifications, hiring data breach lawyers, and the potential law suits that may follow.

It is too soon to tell if this tactic will prove fruitful, but this is definitely something we will need to keep an eye on going forward.



Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: https://www.bleepingcomputer.com/news/security/allied-universal-breached-by-maze-ransomware-stolen-data-leaked/