CASE STUDY

Facing Down a Successful Ransomware Attack

Manufacturer Turns to Conversant Group for Incident Response

CLIENT DETAILS

COMPANY
Manufacturer in the Southern U.S.

OPERATIONS
Global

IT ENVIRONMENT
Approximately 150 servers and desktops

OT ENVIRONMENT
HVAC, building maintenance, IIoT and IoT devices

REVENUE
Approximately $90 million annually

BUSINESS IMPACT AVERTED

500 staff hours of manually recompiling and entering missing ERP data

60,000 staff hours to reproduce 40 years of lost IP designs

Many business executives believe successful cyberattacks only happen to other businesses and not to their companies. When Conversant Group was engaged by a manufacturer based in the United States this was the mindset of their entire management team. Aware of the company's deficiencies, the IT Director secured approval for an abridged security posture assessment—engaging Conversant Group in January 2018.

The assessment pinpointed a laundry list of cybersecurity and disaster recovery deficiencies and argued they represented impending risk. "Among other things, the assessment found that the firewall was from the same vendor as the company's traditional endpoint security solution, which only included traditional signature-based protection," recalls John Anthony Smith, the Founder, President, and Chief Listening Officer of Conversant Group.

REENGAGED, BLUNT FINDINGS PRESENTED TO THE BOARD

When IT was placed under the VP of Plant Operations in late 2018, Conversant Group was reengaged to create a more detailed risk assessment report. Smith was asked to present the findings to the Board of Directors in March 2019. "I presented our findings in very blunt terms to the board," he says. "I told them that based on their very limited number of mitigating security controls, they likely had already been hacked. And if they had not been, they would be very soon."

Unlike the response to the earlier assessment, the Board of Directors took action, purchasing Fortinet FortiGate next-generation firewalls (NGFWs) and Alert Logic Essentials. The latter was recommended due to its ability to extend endpoint protection beyond pattern-based signatures (traditional antivirus) to artificial intelligence (AI) capabilities.

Unfortuantely, before the technologies were fully put into place, Smith's prophetic conclusions would be proven true.

Brandon Williams, Conversant Group's Chief Operating Officer, remembers the state of affairs: "Their security practices were weak, and they weren't postured very well to prevent outsiders from gaining access. If a list of things they shouldn't be doing existed, they were doing most of them. And to top it off, the executive management team truly believed they could go back to pencil and paper without any interruption to the business."

MR.DEC EXECUTED

Almost two weeks after Smith's presentation to the board, he was about to follow up on the board's review of his recommendations. But before he could do so, his team received a severity one (emergency) call from the manufacturer's IT Director at 6:45 AM. The company's shipping and receiving manager arrived at work to discover her computer locked and displaying a ransomware message: "You are unlucky. The terrible virus has captured your files. For decoding, please contact email at @ protonmail.com."

The shipping and receiving manager alerted the IT Director, who immediately called Conversant Group. He reached the on-call support specialist, who told him to disconnect every machine from the internet and to ensure no one turned on their machines. Smith then got his staff in motion, with several forensics analysts and incident response specialists arriving within an hour of the IT Director's call. Members of Conversant Group's executive management team arrived on site, and a "war room" was set up for their Computer Security Incident Response Team (CSIRT).

Keith Weber, a cybersecurity engineer and ethical hacker, was one of the first members of the Conversant Group team to arrive. "We didn't identify the malware until about 8:30 AM, which we determined was a variant of Mr.Dec ransomware pack. It was a known virus, having been in the wild since late 2017."

The finding was a bit disconcerting to the Conversant Group team because Mr.Dec uses the 256-bit Advanced Encryption Security (AES) algorithm to encode files. "It virtually encrypts any useful file types, and without the keys to decrypt the file, it is virtually impossible to break it," Weber explains. Forensic analysis also led Conversant Group to the first known machine in the chain of encrypted devices. "The attack was executed at 9:59 PM on April 1 through a domain account and and communicated over the network using port 3389," Weber continues. "Because the cyber criminals had control of a domain account and the remote desktop

POST-INCIDENT TECHNOLOGY IMPLEMENTATION

FIREWALL
Fortinet FortiGate Next-Generation Firewall

ENDPOINT PROTECTION
Alert Logic Essentials, Fortinet FortiClient, Avecto Defendpoint, Cisco Umbrella

EMAIL SECURITY
Mimecast Advanced Email Security, Mimecast Message Control Suite

BACKUP AND RECOVERY
Unitrends Recovery Backup Appliance, HPE Nimble Storage Appliance

SECURE ACCESS
Cisco Meraki, Citrix Virtual Apps and Desktops

NETWORK INSPECTION
Alert Logic Essentials, Darktrace Enterprise

SECURITY OPERATIONS CENTER
Artic Wolf CyberSOC Service

Mr.Dec Ransomware Timeline

Pre-Jan. 19 First Hacking Event

Attacker—which appears different than the one associated with Mr.Dec—accesses internal user mailbox with a compromised password. Samples and marketing materials that could be reproduced only with reverse-engineered machines begin to appear from overseas competitors.

Jan. 19 to March 19
Second and Third Hacking Events

Early Jan — Spear-phishing email campaign successfully allows attackers to gain remote control of several user workstations, comprises a targeted email account, and gains domain-level administrative access.

Late March — Due to the lack of lateral east-west inspection tools, The attacker begins begins to move laterally across network infecting Windows devices using Remote Desktop Protocol (RDP) over port 3389.

port, they had the keys to the kingdom and could do whatever they wanted on the network."

MAPPING OUT A FORENSICS TRAIL

The forensics analysis proved difficult. "They had no PCAP (packet capture) files, no IPS (intrusion prevention system) logs, no IDS (intrusion detection system) logs—the bread crumbs needed to identify how the attack had gotten into the company's network and where it may have originated from," Weber notes.

The one saving grace is that Conversant Group had set up the FortiGate NGFW before the attack commenced. "It was in listen mode only, as it hadn't been deployed into full production, and thus it wasn't blocking abnormal connections," Weber says. "However, we were able to use the FortiGate NGFW to get a better understanding of the egress and ingress connections within that two-week timeframe with timestamps, which was a huge help in the investigation process," Weber says. "We quickly concluded that the network was a mess. They had employees bringing in their own computers, and Internet-of-Things (IoT) devices and random Wi-Fi connections were everywhere."

Business Impact Analysis Critical to Risk Tolerance

When Conversant Group conducts a cybersecurity risk assessment for a client, the process typically starts with a Business Impact Analysis (BIA). "We believe that you must understand what is really critical to your business before you can pinpoint risk tolerance," says Shayne Champion, the CISO at Conversant Group.

As the Conversant Group CSIRT conducted a full forensics investigation of the manufacturer's environment, the team estimated that about 60-plus percent of the Windows-based machines on the network had been infected and encrypted. Yet, identification of infected systems was significantly impaired by the lack of accurate device and hardware inventories. According to Shayne Champion, the Chief Information Security Officer (CISO) at Conversant Group, this posed a major problem. "Accurate and updated inventories of systems are critical during any incident response," Champion explains. "If businesses don't know what systems they have, what kinds of devices are in their environments and where they are at, and what software is running on them, businesses are far less likely to detect cyberattacks and, in the event of an intrusion, to determine the extent of the impact."

As the Conversant Group CSIRT team conducted their investigation, they found clear indicators that the ransomware was not the first attack the company had suffered. "The client had likely been hacked three times," Smith recounts. "They had marketing materials that had been replicated almost verbatim by a company based in Asia." For the ransomware attack, Smith's team determined the execution came through two compromised IP addresses in Denver, Colorado and China.

One upside of the attack is that Mr.Dec only affects Windows machines, and thus neither the manufacturer's Programmable Logic Controllers (PLC) nor its Supervisory Control and Data Acquisition (SCADA) systems were impacted. The cyber criminals also made a mistake in their attack chain sequence. "While they were using an elevated domain account to move laterally across the network to infect other machines, they infected and encrypted the domain controllers," Weber explains. "As a result, the malicious behavior was noticed more quickly and their access to communicate with other machines on the network was shut down. Had this not occurred, the attackers would likely have compromised 100 percent of the devices on the network."

BACKUP AND DR PROCESSES FLAWED

Under normal circumstances where systems and data had been encrypted, Conversant Group would simply work with the customer to enact their backup recovery processes. In this scenario, the customer only loses a day or two of data.

But Conversant Group and the customer quickly discovered the backup was flawed. "We had a Barracuda backup appliance," says the IT Director. "However, in addition to the backup and recovery processes being excruciatingly time consuming, they also could be messed up very easily." And that is precisely what had happened. One of the plant operations staff accidentally moved a database out of the backup path due to the storage device running out of space. The result is that the customer had no backups for its critical Epicor ERP (Enterprise Resource Planning) or Windchill PLM (Project Lifecycle Management) systems.

In the case of Epicor, the latest backup copy was two months old. The manufacturer would have lost two months of data, and administrative staff would

Mr.Dec Ransomware Timeline

Day 0, April 1

Attack commences at 9:49 PM. Approximately 60-plus percent of Windows machines are encrypted using Advanced Encryption Standard (AES).

Day 1, April 2

6:30 AM — Shipping and Logistics Manager arrives and discovers ransomware message on her computer.

6:45 AM — Company IT Director contacts Conversant Group helpdesk for assistance.

7:00 AM — All systems disconnected from internal network and external internet access is disabled.

7:45 AM — First consultant from Conversant Group arrives on site.

8:30 AM — Conversant Group forensics analyst identifies the malware as a Mr.Dec ransomware variant.

8:45 AM — Conversant Group forensics determines domain account called "ASP" is distributing ransomware payload.

9:30 AM — Conversant Group CSIRT initiates triage process for client endpoints.

Mr.Dec Ransomware Timeline

Day 1, April 2	
4:00 PM	CSIRT works with company to determine that backups for critical corporate systems are incomplete.
8:25 PM	CSIRT begins communicating with cyber criminals over secure email system; files submitted to verify threat actors have decryption capability.
8:45 PM	CSIRT estimates that about 60-plus percent of endpoints were compromised.
10:00 PM	Conversant Group sets up dedicated CSIRT "war room."
Day 2, April 3	
1:45 AM	Bitcoins used to pay ransom for decryption key.
6:10 AM	Encryption key sent by cyber criminals; Conversant Group discovers that encryption key pairs are unique for each endpoint. Learns RDS was being used for distribution.
9:00 AM	Conversant Group CISO delivers briefing to all company employees, explaining cause for business disruption, providing perspective and clarity to dispel rumors, and answering questions.

have needed to expend upwards of 500 staff hours manually recompiling and entering the missing data. The situation with Windchill was dramatically more serious. The manufacturer would have lost 40 years of intellectual property designs that would have taken years of staff hours to reproduce—if that was even possible. Initial estimates ranged in the vicinity of 60,000 staff hours.

PAYING THE BITCOIN RANSOM

The Mr.Dec ransomware provided a unique identifier on the screen of every infected machine and required a payment in Bitcoin cryptocurrency to decrypt each device. "You never want to pay a ransom if there is any way around doing so, as there is no guarantee that the cyber criminals will actually provide decryption keys once paid," Champion notes. However, due to deficient backup systems and processes, after a meeting between the executive management team, the IT Director, and Conversant Group at 9 PM, a decision was made to pay the Bitcoin ransom for a decryption key.

The Conversant Group CSIRT began communicating with the cyber criminals using the open-source encrypted email platform ProtonMail. "We created a ProtonMail account to initiate contact with them," Weber says. "It was immediately clear we were dealing with foreign threat actors, their communications read as if they were using Google Translator to communicate with us in English."

Conversant Group wanted proof that the cyber criminals could decode the encrypted machines, and they selected two files from the laptop of the IT Director and sent them over the ProtonMail account. A couple of hous later, the decrypted files were sent back. "A decision was made to pay the ransom and we remitted Bitcoins into the

Disguised in a Name

The username the attackers employed on the domain account was labeled ASP, a common service used in Microsoft .NET environments. Other accounts were using other common Microsoft service account names. By using these common Microsoft nomenclatures and only adding the accounts to the built-in/ administrative group, the attackers cleverly disguised their attack from immediate notice.

account of the cyber criminals," Weber recounts. "They asked us to send them a screen shot as proof."

While the two teams waited on a response, they met in the war room to plot out steps for the next day (Day 2). While the company's executive management team wanted tightly controlled communications, Champion argued for the value of transparent communications with all employees. The executive management team was persuaded and elected to have Champion present to and answer questions from employees at 9 AM the next morning.

With a strategic plan in place, the bulk of the team went home to get some sleep, leaving several members of Conversant Group to wait on a response from the cyber criminals. The decryption keys arrived shortly after 4 AM, but when they tried to use them on machines other than the IT Director's laptop, they discovered each infected machine required its own unique key.

DECRYPTING AND REBUILDING EPICOR AND WINDCHILL

Champion presented at an employee all-hands meeting at 9:00 AM in the morning and fielded a number of questions from the staff. "A ransomware attack can be terrifying for a company that hasn't experienced one," Champion notes. "But I explained that it actually isn't that frightening; companies go through it every day. I told them the steps we were going through, what we knew, and didn't know." His communication was received very well, and he was asked twice more over the next 12 days to update them on the team's progress."

> **"In all, we exchanged 42 different emails with the cyber criminals over ProtonMail."**
>
> Keith Weber, Cybersecurity Engineer and Ethical Hacker, Conversant Group

Following the all-hands meeting, the team determined that it would need to purchase more Bitcoins to recover critical data for the Epicor and Windchill systems. They concluded the Epicor server was the most crucial piece to get back up, and they began communicating with the threat actors again and sent them more Bitcoins at 2 PM. It wasn't until 1 AM the next day (Day 3) that the decryption keys arrived, and the Conversant Group team began rebuilding the database in concert with the Epicor support team on isolated servers..

Additional Bitcoins were sent for the decryption of Windchill files at 2 AM on April 6 (Day 5), but when Conversant Group ran

Mr.Dec Ransomware Timeline

Day 2, April 3

10:00 AM	Additional Fortinet FortiGate NGFW is placed in-line to enable access for additional remote Conversant Group team members and to provide additional network security.
10:30 AM	CSIRT utilizes forensic live disk tools to identify Indicators of Compromise (IOCs) on systems infected with ransomware. All printers and other network devices manually checked to ensure they are disconnected from Local Area Network (LAN).
11:00 AM	CSIRT starts reverse engineering ransomware using Ghidra tool from the National Security Administration (NSA).
1:20 PM	Encrypted Epicor ERP files submitted for decryption key.
2:20 PM	Client pays additional Bitcoins to ensure restoration of business-critical Epicor data.
3:00 PM	Two additional unauthorized accounts (ADMIN$ and ADMIN$$) identified with domain administrative privileges, with forensics determining that accounts had been created as early as four months before Mr.Dec attack commenced.

Mr.Dec Ransomware Timeline

Day 2, April 3

5:00 PM — CSIRT meets with company leadership team for first end-of-day "hot wash" review.

6:30 PM — CSIRT team members use Alert Logic Extended Endpoint Protection and open-source, pattern-based anti-virus programs to validate clean systems.

Day 3, April 4

1:00 AM — Decryption keys for Epicor received; system rebuild commences.

2:00 PM — Investigation of office workstations reveals that emails sent to user who frequently travels to Asia has exhibited odd behavior. Forensics determines user's Office 365 account had been compromised for months. Further forensics uncovers two additional compromised Office 365 accounts.

CSIRT finishes manual process to inventory all infected endpoints.

3:30 PM — Systems for key employees are restored and brought back online.

5:00 PM — CSIRT leads "hot wash" review meeting and sets priorities for activities based on the company's business needs.

the decryption key it failed. "We notified them over the ProtonMail account and things went silent until early the next day (Day 6)," Weber says. "Then, they came back and indicated that we should mount the drive on a separate machine and run the decoder. At the same time, they told us that if we have a problem, they would be more than happy to remote in and help us fix it. This was one of the funniest things I've ever read."

ALIGNING CYBER SECURITY AND BUSINESS STRATEGY

In accordance with incident response best practices, Conversant Group initiated "hot wash" meetings—where CSIRT leaders met at the end of each day with the manufacturer's management team to discuss progress made and obstacles encountered that day and map out work for the next day. During each hot wash, the management team communicated with the CSIRT to prioritize eradication and system recovery activities. However, as the CSIRT worked to restore individual workstations and business-critical systems, the team was continually pulled back and re-tasked—creating inefficiencies in the progress of restoring the company to normal operations.

> **"We had successfully deployed Alert Logic onto a handful of endpoints prior to the incident, and none of those were infected. Had we been able to get it onto all of our endpoints, we likely would have prevented the attack."**
>
> IT Director

During the Day 4 hot wash session, it became clear that the company understood neither the interaction of all its systems nor the overall value of these business processes in the context of corporate goals. In response, Champion stopped the hot wash and asked the company's leadership team to list each discrete business unit. Once they had done so, he asked them to list every major software program used by each one. The resulting chart, which Champion created on a Post-It easel pad, enabled them to visually identify business-critical systems from the perspective of both the business and individual leadership members. The result enabled the CSIRT to align each prioritized activity with a measurable business objective. leadership team to pinpoint what department was missing from the list. They scrutinized the list and concluded it was complete, until Champion noted that Information Technology (IT) was not included. “While they are a manufacturer, I explained to them that their business could not function without the IT Department,” Champion notes. “Instead, IT and cybersecurity should be seen as critical enabling functions and key differentiators for their manufacturing processes.”

Getting the Right Technologies in Place

As the prior backup and recovery solution was not a usable option, Conversant Group worked with the IT Director to implement new technologies. The Barracuda backup appliance was replaced with a Unitrends Recovery Backup Appliance. In addition, the HPE legacy storage arrays were upgraded by migrating to a HPE Nimble Storage Appliance. “With the new Nimble and Unitrends solutions in place, daily backups take 20 to 30 minutes compared to 11 or 12 hours with the prior configuration,” says the company’s IT Director.

While the manufacturer had purchased Alert Logic Essentials (formerly Barkly), the IT Director had been unable to deploy it onto but a handful of endpoints in the short time since it had been acquired—and those were operating in monitor-only mode. Additionally, the company had been unable to uninstall its Sophos endpoint security so that it could install Fortinet FortiClient endpoint protection on its endpoints. “Unfortunately, Sophos doesn’t offer an uninstall script, and we found ourselves stuck trying to figure out how to remove it from endpoints so we could install FortiClient on them,” the IT Director says. “When the Mr.Dec attack commenced, Sophos failed to detect or prevent the attack. It proved to be a dismal failure, with Mr.Dec or the attacker literally eating the Sophos software. We couldn’t even get into a console.”

To solve the problem, consultants from Conversant Group had to remove Sophos manually from each machine and then deploy FortiClient and Alert Logic in its place. They also added Mimecast Advanced Email Security and MessageControl CodeBreaker and Silencer to protect the company’s cloud-based Office 365 environment. “The manufacturer previously relied on the default security built into Microsoft Office 365,” Champion says. “It is widely known that this built-in capability is inadequate. With over 90 percent of successful cyberattacks coming via email, having a robust, proactive mail security solution is a requisite.”

Conversant Group also deactivated the manufacturer’s Sophos firewall and migrated the FortiGate NGFW from listening mode

Mr.Dec Ransomware Timeline

Day 4, April 5

10:00 AM — Restoration begins for network-based Voice over IP (VoIP) phone system.

3:30 PM — CSIRT continues triage for all endpoint systems.

5:00 PM — During the daily “hot wash” meeting, CSIRT leads company leadership to scope business processes and systems used to establish restoration prioritization.

Day 5, April 6

2:00 AM — Encrypted Windchill files submitted for decryption key along with two Bitcoins.

9:00 AM — CSIRT continues to contain and eradicate malware—including the re-imaging of some endpoints.

2:00 PM — Unitrends Recovery Backup Appliance fully deployed and placed in production.

5:00 PM — Error received when decryption of Windchill files was attempted.

Day 6, April 7

2:00 AM — Cybercriminals indicate they must mount Windchill drive on a separate machine and offer to “remote into company systems to help.”

10:00 AM — Process begins to rejoin all endpoints to the company domain.

Mr.Dec Ransomware Timeline

Day 7, April 8

8:00 AM — Fortinet FortiClient implemented to protect endpoints and automate protective actions based on threat intelligence.

10:00 AM — Conversant Group implements Printer Logic to centrally manage printers.

2:00 PM — Epicor modules fully rebuilt and online (Shipping, HR, Finance, and Engineering).

4:00 PM — CSIRT implements least-privilege user access for files on Storage Area Network (SAN).

6:00 PM — Windchill database fully restored and application placed back online.

10:00 PM — Conversant Group implements PDQ Deploy to assist client in end-user software deployment and management.

Day 9, April 10

9:00 AM — HPE Nimble Storage Appliances deployed and in production.

Day 14, April 15

9:00 AM — Mimecast Email Security with Targeted Threat Protection (TTP) deployed and in production.

> **“An emergency such as this ransomware attack can bring to light what is important in your company. This is exactly what happened in this instance, and Conversant Group played a critical role in guiding us to a successful completion.”**
>
> IT Director

into production to activate its advanced capabilities—IPS, web filtering, firewall, and Secure Sockets Layer (SSL)/Transport Layer Security (TLS) inspection. “Being able to inspect encrypted traffic is critical,” Champion says. “In this instance, through our forensics analysis, the cyber criminals used encryption to infiltrate the network. Without SSL/TLS inspection, it becomes immensely harder to detect and prevent these types of malicious attacks.”

To further secure access to the internet, Conversant Group deployed Cisco Umbrella. “We are able to leverage the Cisco Threat Intelligence through the Cisco DNS to proactively manage to what our users connect to on and off our network,” says the IT Director. Previously, users could connect virtually any device to the network, including rogue access points and IoT devices without any approval process.

“Shadow IT is also a real problem for us, where employees would connect virtually anything to the network,” he continues. “But using using the combination of the Cisco and FortiGate NGFWs, we are able to manage that umbrella process much more much more tightly.” In addition, consultants from Conversant Group worked with the IT Director to develop and provide a cybersecurity awareness training program to educate employees on security best practices.

“We also worked with their team to implement Two-Factor Authentication (2FA), including regular password updates,” Williams adds. “All of the users also had local administrative rights, which created significant risk exposure. This is all changed now. We implemented Avecto Defendpoint to prevent users from executing unapproved code on endpoints while elevating those applications that require administrative rights to properly function.”

Understanding Lollipop Security

Historically, security consultants compare security to an onion. Smith abhors the analogy, claiming a lollipop with different candied layers and a Tootsie Roll or bubblegum at the center is more appropriate. "An onion smells and the more layers you peel back, you eventually get to nothing of value—the center of the onion is gross," he says. "If you look along the lollipop layers, each of the hard layers eventually lead to the center of the candy. In the case of this client, every layer of security was flawed—from the network and firewall, to the backups, to the endpoints. They were very, very lucky that the cyber criminals were nice. They could have taken their money and run, not providing the decryption algorithms we needed to unlock the data."

Ultimately, many of the manufacturer's administrative back-office functions were offline for nine days. This impacted about 100 administrative staff, resulting in upwards of 8,000 lost staff hours. Fortunately, plant operations were not affected, as the manufacturer had just enough orders in the queue that operations were not halted.

"Without the help of Conversant Group, we would never have gotten our systems back online in such a short period of time, and the operational outage would have directly impacted revenue," notes the IT Director. "I don't hire vendors that know what I know. I look for vendors that add value."

He continues: "Conversant Group actually taught us how to work better as a team. Their communications structure—from the lowest person in the organization to the President—facilitates collaboration and thinking outside the box. You wouldn't necessarily think a situation like this could be viewed as a positive, but it was for us. Not only did it help align our IT strategy with our business objectives, but it created a more cohesive team. Everyone now believes that IT is a strategic part of the business instead of a helpdesk."

> **"If you look at the layered 'lollipop' model, each of the hard candied layers eventually leads to the center of the candy. In the case of this client, every layer of security was flawed—from the network and firewall, through the backups, and all the way to the endpoints. They were very, very lucky that the cyber criminals were nice."**
>
> John Anthony Smith,
> Chief Listening Officer and
> President, Conversant Group

CLIENT RECOMMENDATIONS

1. Contain the outbreak by disconnecting all switches, servers, and access points.

2. Understand what data and systems are critical and must be restored.

3. Backups are one thing. EEnsure that data can be recovered and systems can be quickly and easily restored.

4. Ensure all hardware (such as storage systems) are under maintenance.

5. Build a culture of security, which begins with user awareness.

www.conversantgroup.com
423-305-7890
sales@conversantgroup.com

Conversant Group is an IT infrastructure and security consulting company based in Chattanooga, TN. Conversant Group has provided technical, organizational, procedural, and process consulting internationally since the company was formed in 2009. Unlike many in IT, Conversant Group has a unique perspective: technology is a tool, nothing more. Technology should support the business, and the business should support the people.