# GREENVILLE TECHNICAL COLLEGE SECURITY BREACH 2020

James Nolen


https://www.gvltec.edu/

# Security Breach Timeline

1. Attackers gained access to GTC's network (Unknown Date, 2020).
2. Attackers exfiltrated approximately 600GB of data from affected servers, workstations, and storage (Unknown Date, 2020).
3. Attackers initiated their ransomware, encrypting the impacted servers, workstations, and storage (August 2020).
4. GTC discovered the malware infection affecting their systems (August 27, 2020).
5. GTC publicly announced a potential security incident (August 28, 2020).
6. Avaddon claimed responsibility for the attack (August 29, 2020).
7. GTC acknowledged the credibility of the attack and the extent of the data breach (September 1, 2020).
8. System Disruption Update provided recommendations for victims and acknowledged the data breach (October 23, 2020).
9. GTC's Board acknowledged the breach, leading to financial repercussions and project delays (January 20, 2021).
10. FBI informed GTC that the investigation is ongoing, and progress has been made in identifying the ransomware attackers (November 16, 2022).

# Avaddon Ransomware Mapped with Mitre Att@ck

**Initial Access: Attackers gained access to GTC's network (Unknown Date, 2020).**

- Unknown Technique

**Execution: Attackers establish a foothold within GTC's network using exploits in GTC's network vulnerabilities (Unknown Date, 2020).**

- T1106: Native API
- T1047: Windows Management Instrumentation

**Persistence: Attackers maintain foothold within GTC's network (Unknown Date, 2020).**

- Unknown Technique

**Privilege Escalation: Attackers escalated their privileges (Unknown Date, 2020).**

- Unknown Technique

**Defense Evasion: Attackers evade detection (Unknown Date, 2020).**

- T1140: Deobfuscate/Decode Files or Information
- T1112: Modify Registry
- T1027: Obfuscated Files or Information

**Credential Access: Attackers may have accessed credentials during the lateral movement and privilege escalation stages (Unknown Date, 2020).**

- Unknown Technique

**Discovery: Attackers identify and assess GTC's systems, network configuration, and vulnerabilities (Unknown Date, 2020).**

- T1083: File and Directory Discovery
- T1135: Network Share Discovery
- T1057: Process Discovery
- T1016: System Network Configuration Discovery

**Lateral Movement: Attackers laterally moved within GTC's network using exploits in GTC's vulnerabilities (Unknown Date, 2020).**

- Unknown Technique

**Collection: Attackers exfiltrated approximately 600GB of data from affected servers, workstations, and storage (Unknown Date, 2020).**

- Unknown Technique

**Command and Control: Attackers maintain communication with their C2 infrastructure to facilitate continuous control of the victim's environment (Unknown Date, 2020).**

- Unknown Technique

**Exfiltration: Attackers exfiltrated approximately 600GB of data (Unknown Date, 2020).**

- Unknown Technique

**Impact: Attackers initiated their ransomware, which caused the impacted servers, workstations, and storage to be encrypted (August 2020).**

- T1486: Data Encrypted for Impact
- T1490: Inhibit System Recovery
- T1489: Service Stop

https://attack.mitre.org/software/S0640/

# Avaddon Ransomware Mapped by Mitre Att@ck

**about**
Avaddon Ransomware

Threat Actor for Greenville Technical College incident 2020

**domain**
Enterprise ATT&CK v12

**platforms**
Linux, macOS, Windows, Network, Containers, Office 365, SaaS, Google Workspace, IaaS, Azure AD

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Command and Control | Exfiltration | Impact |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Drive-by Compromise | Command and Scripting Interpreter | Account Manipulation | Abuse Elevation Control Mechanism | Abuse Elevation Control Mechanism | Adversary-in-the-Middle | Account Discovery | Exploitation of Remote Services | Adversary-in-the-Middle | Application Layer Protocol | Automated Exfiltration | Account Access Removal |
| Exploit Public-Facing Application | AppleScript | BITS Jobs | Bypass User Account Control | Bypass User Account Control | Brute Force | Application Window Discovery | Internal Spearphishing | Archive Collected Data | Communication Through Removable Media | Data Transfer Size Limits | Data Destruction |
| External Remote Services | JavaScript | Boot or Logon Autostart Execution | Elevated Execution with Prompt | Elevated Execution with Prompt | Credentials from Password Stores | Browser Bookmark Discovery | Lateral Tool Transfer | Audio Capture | Data Encoding | Exfiltration Over Alternative Protocol | Data Encrypted for Impact |
| Hardware Additions | Network Device CLI | Active Setup | Setuid and Setgid | Setuid and Setgid | Exploitation for Credential Access | Cloud Infrastructure Discovery | Remote Service Session Hijacking | Automated Collection | Data Obfuscation | Exfiltration Over C2 Channel | Data Manipulation |
| Phishing | PowerShell | Authentication Package | Sudo and Sudo Caching | Sudo and Sudo Caching | Forced Authentication | Cloud Service Dashboard | Remote Services | Browser Session Hijacking | Dynamic Resolution | Exfiltration Over Other Network Medium | Defacement |
| Replication Through Removable Media | Python | Kernel Modules and Extensions | Access Token Manipulation | Access Token Manipulation | Forge Web Credentials | Cloud Service Discovery | Replication Through Removable Media | Clipboard Data | Encrypted Channel | Exfiltration Over Physical Medium | Disk Wipe |
| Supply Chain Compromise | Unix Shell | Login Items | Boot or Logon Autostart Execution | BITS Jobs | Input Capture | Cloud Storage Object Discovery | Software Deployment Tools | Data from Cloud Storage | Fallback Channels | Exfiltration Over Web Service | Endpoint Denial of Service |
| Trusted Relationship | Visual Basic | LSASS Driver | Active Setup | Build Image on Host | Modify Authentication Process | Container and Resource Discovery | Taint Shared Content | Data from Configuration Repository | Ingress Tool Transfer | Scheduled Transfer | Firmware Corruption |
| Valid Accounts | Windows Command Shell | Port Monitors | Authentication Package | Debugger Evasion | Multi-Factor Authentication Interception | Debugger Evasion | Use Alternate Authentication Material | Data from Information Repositories | Multi-Stage Channels | Transfer Data to Cloud Account | Inhibit System Recovery |
| | Container Administration Command | Print Processors | Kernel Modules and Extensions | Deobfuscate/Decode Files or Information | Multi-Factor Authentication Request Generation | Domain Trust Discovery | | Data from Local System | Non-Application Layer Protocol | | Network Denial of Service |
| | Deploy Container | Re-opened Applications | Login Items | Deploy Container | Network Sniffing | File and Directory Discovery | | Data from Network Shared Drive | Non-Standard Port | | Resource Hijacking |
| | Exploitation for Client Execution | Registry Run Keys / Startup Folder | LSASS Driver | Direct Volume Access | OS Credential Dumping | Group Policy Discovery | | Data from Removable Media | Protocol Tunneling | | Service Stop |
| | Inter-Process Communication | Security Support Provider | Port Monitors | Domain Policy Modification | Steal Application Access Token | Network Service Discovery | | Data Staged | Proxy | | System Shutdown/Reboot |
| | Native API | Shortcut Modification | Print Processors | Execution Guardrails | Steal or Forge Authentication Certificates | Network Share Discovery | | Email Collection | Remote Access Software | | |
| | Scheduled Task/Job | Time Providers | Re-opened Applications | Exploitation for Defense Evasion | Steal or Forge Kerberos Tickets | Network Sniffing | | Input Capture | Traffic Signaling | | |
| | Serverless Execution | Winlogon Helper DLL | Registry Run Keys / Startup Folder | File and Directory Permissions Modification | Steal Web Session Cookie | Password Policy Discovery | | Screen Capture | Web Service | | |
| | Shared Modules | XDG Autostart Entries | Security Support Provider | Hide Artifacts | Unsecured Credentials | Peripheral Device Discovery | | Video Capture | | | |
| | Software Deployment Tools | Boot or Logon Initialization Scripts | Shortcut Modification | Hijack Execution Flow | | Permission Groups Discovery | | | | | |
| | System Services | Browser Extensions | Time Providers | Impair Defenses | | Process Discovery | | | | | |
| | User Execution | Compromise Client Software Binary | Winlogon Helper DLL | Disable Cloud Logs | | Query Registry | | | | | |
| | Windows Management Instrumentation | Create Account | XDG Autostart Entries | Disable or Modify Cloud Firewall | | Remote System Discovery | | | | | |
| | | Create or Modify System Process | Boot or Logon Initialization Scripts | Disable or Modify System Firewall | | Software Discovery | | | | | |
| | | Event Triggered Execution | Create or Modify System Process | Disable or Modify Tools | | System Information Discovery | | | | | |
| | | External Remote Services | Domain Policy Modification | Disable Windows Event Logging | | System Location Discovery | | | | | |
| | | Hijack Execution Flow | Escape to Host | Downgrade Attack | | System Language Discovery | | | | | |
| | | Implant Internal Image | Event Triggered Execution | Impair Command History Logging | | System Network Configuration Discovery | | | | | |
| | | Modify Authentication Process | Exploitation for Privilege Escalation | Indicator Blocking | | System Network Connections Discovery | | | | | |
| | | Office Application Startup | Hijack Execution Flow | Safe Mode Boot | | System Owner/User Discovery | | | | | |
| | | Pre-OS Boot | Process Injection | Indicator Removal | | System Service Discovery | | | | | |
| | | Scheduled Task/Job | Scheduled Task/Job | Indirect Command Execution | | System Time Discovery | | | | | |
| | | Server Software Component | Valid Accounts | Masquerading | | Virtualization/Sandbox Evasion | | | | | |
| | | Traffic Signaling | | Modify Authentication Process | | | | | | | |
| | | Valid Accounts | | Modify Cloud Compute Infrastructure | | | | | | | |
| | | | | Modify Registry | | | | | | | |
| | | | | Modify System Image | | | | | | | |
| | | | | Network Boundary Bridging | | | | | | | |
| | | | | Obfuscated Files or Information | | | | | | | |

https://attack.mitre.org/software/S0640/

# Insufficient Security Measures

- Greenville Tech's cybersecurity program had weak protections in place, making it easier for hackers to access sensitive information.

*"The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards." - Gene Spafford, Computer Security Expert*

# Addressing Insufficient Security Measures

- Regular software updates and patch management
- Implement multi-factor authentication (MFA)
- Regular employee training and awareness programs

*"Passwords are like underwear: don't let people see them, change them very often, and don't share them with strangers." - Chris Pirillo, Technology Blogger and Entrepreneur*

# Inadequate Monitoring and Detection

- Greenville Tech's systems lacked effective monitoring and detection tools, making it difficult to identify potential threats and breaches early.

*"There are two types of companies: those that have been hacked, and those that will be." - Robert Mueller, Former FBI Director*

# Addressing Inadequate Monitoring and Detection

- Implement a Security Information and Event Management (SIEM) system
- Conduct regular vulnerability assessments and penetration tests
- Establish a 24/7 security operations center (SOC)

# Limited User Access Control

- Greenville Tech had inadequate user access controls, allowing unauthorized users to access sensitive information more easily.

*"If you spend more on coffee than on IT security, you will be hacked. What's more, you deserve to be hacked." - Richard Clarke, Author and National Security Expert*

# Addressing Limited User Access Control

- Implement the principle of least privilege (POLP)
- Regularly review and update user access permissions
- Use role-based access control (RBAC) to manage permissions

# Insufficient Incident Response Plan

- Greenville Tech did not have a well-defined incident response plan, leading to slower and less effective actions during the security breach.

*"There are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns—the ones we don't know we don't know." - Donald Rumsfeld, Former U.S. Secretary of Defense*

# Addressing Insufficient Incident Response Plan

- Develop a comprehensive incident response plan
- Establish an incident response team (IRT)
- Conduct regular incident response drills and exercises

# Repercussions of Greenville Tech's Security Breach

- Identity theft and fraud risks for affected individuals
- Loss of trust in the institution
- Financial costs for breach response and mitigation
- Legal liabilities and potential lawsuits
- Damage to Greenville Tech's reputation


https://cloudtweaks.com/2017/10/lighter-side-cloud-money-grab/

# Limiting Damage from Repercussions

- Provide identity theft protection and credit monitoring services to affected individuals
- Transparent communication and public relations efforts to rebuild trust
- Collaborate with law enforcement to track down the perpetrators

# Thank You and Contact Information

Thank you for your time! If you have any questions or comments about this presentation or cybersecurity, please reach out to me.

James Nolen

nolenjgn@my.gvltec.edu

github.com/jgnolen

linkedin.com/in/jgnolen

# References


- MITRE. (n.d.). S0640. Retrieved April 1, 2023, from https://attack.mitre.org/software/S0640/
- Greenville Technical College. (n.d.). Data and Event Calendar. Archived from the original on June 25, 2021. Retrieved April 1, 2023, from https://web.archive.org/web/20210625035634/https://www.gvltec.edu/about_greenvilletech/administration_governance/data-event.html
- DataBreaches.net. (2020, August 31). Greenville Technical College claims no personal data affected by ransomware incident; threat actors claim otherwise. Retrieved April 1, 2023, from https://www.databreaches.net/greenville-technical-college-claims-no-personal-data-affected-by-ransomware-incident-threat-actors-claim-otherwise/
- Brown, E. (2020, September 1). Greenville Tech backtracks, calls data breach 'credible threat'. Greenville News. Retrieved April 1, 2023, from https://www.greenvilleonline.com/story/news/local/2020/09/01/greenville-tech-backtracks-calls-data-breach-credible-threat/3453854001/
- HackNotice. (n.d.). Greenville Technical College (GTC) Ransomware Attack Data Incident. Retrieved April 1, 2023, from https://app.hacknotice.com/#/hack/5f49650e2ac74f1a4f91a1c9
- Brown, E. (2020, August 28). Greenville Tech says it thwarts data breach after ransom sought. Greenville News. Retrieved April 1, 2023, from https://www.greenvilleonline.com/story/news/local/2020/08/28/greenville-tech-says-thwarts-data-breach-after-ransom-sought/5662602002/
- Audacy. (2021, September 21). Cybersecurity breach at GTC. WORD-FM. Retrieved April 1, 2023, from https://www.audacy.com/989word/articles/news/cybersecurity-breach-at-gtc
- Cimpanu, C. (2021, July 12). Avaddon ransomware operation shuts down and releases decryption keys. The Record. Retrieved April 1, 2023, from https://therecord.media/avaddon-ransomware-operation-shuts-down-and-releases-decryption-keys/
- Williams, T. (2021, July 12). Avaddon ransomware shuts down and releases decryption keys. Bleeping Computer. Retrieved April 1, 2023, from https://www.bleepingcomputer.com/news/security/avaddon-ransomware-shuts-down-and-releases-decryption-keys/
- Williams, T. (2021, July 14). US and Australia warn of escalating Avaddon ransomware attacks. Bleeping Computer. Retrieved April 1, 2023, from https://www.bleepingcomputer.com/news/security/us-and-australia-warn-of-escalating-avaddon-ransomware-attacks/
- Greenville Technical College. (n.d.). 4.04 Information Security Policy. Retrieved April 1, 2023, from https://www.gvltec.edu/about_greenvilletech/administration_governance/admin_policies/4-04-Information-Security-Policy.html
- Greenville Technical College. (2022, January 16). Greenville Technical College Board of Commissioners Meeting Minutes. Retrieved April 1, 2023 from https://www.gvltec.edu/about_greenvilletech/administration_governance/area_commission/minutes-agendas/111622-GTC-board-minutes.pdf
- Greenville Technical College. (n.d.). [Image]. Retrieved April 1, 2023, from https://www.gvltec.edu/campus-life/campus-services/campus-maps/campus-map.html
- CloudTweaks. (2017). The Lighter Side of the Cloud: The Money Grab [Image]. Retrieved from https://cloudtweaks.com/2017/10/lighter-side-cloud-money-grab/
- Adrian Sanchez Hernandez, P. T. (2022, January 19). *One Source to Rule Them All: Chasing AVADDON Ransomware*.[Blog post]. https://www.mandiant.com/resources/blog/chasing-avaddon-ransomware