FOR528: **Ransomware and Cyber Extortion™**

4 Day Program	24 CPEs	Laptop Required

Who Should Attend

- Information security professionals who want to learn how to collect, parse, and analyze forensic artifacts in support of ransomware incident response
- Incident response team members who need to use deep-dive digital forensics to help solve their Windows data breach and intrusion cases, perform damage assessments, and develop indicators of compromise
- Incident triage analysts such as those working in a Security Operations Center, Computer Incident Response Team, or similar
- Managed Services Provider (MSP) and Managed Security Services Providers (MSSPs) analysts who may need to aid in ransomware incident response
- Law enforcement officers, federal agents, and detectives who want to become deep subject-matter experts on ransomware investigations
- Medical and hospitality IT staff who may need to response to ransomware events
- Anyone interested in a deep understanding of Ransomware-specific Incident Response who has a background in information systems, information security, computers

Nice Framework Work Roles

- Cyber Defense Incident Responder (OPM 531)
- Cyber Operator (OPM 321)
- Cyber Crime Investigator (OPM 221)
- Law Enforcement/Counter Intelligence Forensics Analyst (OPM 211)
- Cyber Defense Forensics Analyst (OPM 212)

Course Topics

- Ransomware Evolution and History
- Windows Forensics Artifacts Critical to Ransomware Incident Response
- Evidence Acquisition Tools and Techniques
- Initial Access
- Execution and Defense Evasion
- Persistence
- Privilege Escalation and Credential Access
- Lateral Movement
- Active Directory Attacks
- Data Access
- Data exfiltration
- Archive creation and data staging
- Data exfiltration routes
- Backup and Recovery tampering
- Payload deployment
- Encryption specifics including source code review
- Decryptors
- Cobalt Strike architecture, components, and payloads
- Dealing with an active threat
- Conti ransomware operations case study
- Hunting methods and techniques

Learning to thwart the threat of human-operated ransomware once and for all!

The term “Ransomware” no longer refers to a simple encryptor that locks down resources. The advent of Human-Operated Ransomware (HumOR) along with the evolution of Ransomware-as-a-Service (RaaS) have created an entire ecosystem that thrives on hands-on the keyboard, well-planned attack campaigns. It is a rapidly growing threat that has evolved from being a single machine infection following an ill-advised mouse click to becoming a booming enterprise capable of crippling large and small networks alike. Even when extortion actors do not deploy an encryptor, the fallout can be devastating.

Organizations are at risk of losing their data and information to these attacks, which can lead to revenue losses, reputational damage, theft of employee time and productivity, and inability to function normally. It is now common to see these large-scale, sophisticated attacks where the ransomware actors first establish persistence and execute tools on their target, then move laterally throughout the organization, and ultimately exfiltrate data before deploying their ransomware payloads. That is, if they even deploy an encryptor.

Even though payments to ransomware actors slowed in early 2022 as compared to previous years, that same year there were over 2,600 posts made to extortion sites related to ransomware. This number does not include an unknown quantity of incidents that were resolved through communication and/or negotiation behind the scenes prior to public notification. Of the reported incidents from 2022, the following are the top 10 compromised sectors:

- Construction
- Hospital and Health Care
- Government Administration
- T Services and IT Consulting
- Law Practice
- Automotive
- Financial Services
- Higher Education
- Insurance
- Real Estate

The FOR528: Ransomware and Cyber Extortion course teaches students how to deal with the specifics of ransomware to prepare for, detect, hunt, respond to, and address the aftermath of these attacks. The course features a hands-on approach to learning using real-world data and includes a full day capture the flag (CTF) challenge to help students solidify their learning. The four-day class teaches students what artifacts to collect, how to collect them, how to scale collection efforts, how to parse the data, and how to review the parsed results in aggregate.

The course also provides in-depth details and detection methods for each phase of the ransomware and cyber extortion attack lifecycle. These phases include Initial Access, Execution, Defense Evasion, Persistence, Attacks on Active Directory (AD), Privilege Escalation, Credential Access, Lateral Movement, Data Access, Data Exfiltration, and Payload Deployment.

Unfortunately, many businesses will find themselves falling victims to ransomware attacks because they feel they are not in danger. Regardless of whether your organization is small, medium, or large, every internet-connected network is at risk... and the threat is not going away any time soon.

Section Descriptions

SECTION 1: Ransomware Incident Response Fundamentals

The Ransomware and Cyber Extortion course begins with a review of ransomware's history. We begin with the story of the first-known ransomware attack and work our way to the current-day threats that loom over our industry. Our inner-connected lives, not to mention livelihoods, are at risk everyday thanks to the advent of HumOR and RaaS. You will increase your understanding of ransomware as we deep-dive into the roles, processes, communication methods, and activities related to these threats.

We then cover what to do if you are about to be encrypted, are currently being encrypted, or were just recently encrypted. We cover the actions you need to take including the entities you need to contact, the departments you need to involve, and the processes you need to put in place with special attention to temporal requirements—the clock is ticking!

After learning about the true threats we face and how we can apply incident response practices in general, we begin our deep-dive into the Windows-based forensic artifacts best suited to ransomware campaign analysis. You'll learn which artifacts to collect along with which tools and methods are best suited to acquisition and parsing. Regardless of your organization's level of preparedness, we'll cover what you can do to obtain data that will facilitate analysis.

You'll learn the hands-on approaches for direct acquisition against single machines and then transition to acquisition and analysis at-scale. Detailed hands-on labs walk you through analysis methods for each environment type. You'll use TimeSketch to analyze parsed artifacts, ensuring that you recognize the easy wins and more advanced analysis practices to help you and your organization respond to the ransomware threat.

TOPICS: Course VMs; Review of Our Custom Target Victim and Their Network; Custom Attack Scenarios Overview; Ransomware Evolution and History; Ransomware-as-a-Service (RaaS); Initial Access Brokers (IABs); Ransomware Operators; Dealing with an Active Threat; Ransomware Payments; Ransomware Payments; Forensic Artifact Collection; Incident Response Processes and Their Application to Ransomware; Windows Forensic Artifacts; Analysis at Scale; Analysis at-scale via TimeSketch

SECTION 2: Ransomware Modus Operandi

Ransomware incidents are not especially unique. We incident responders see the same tactics, techniques, and procedures (TTPs) over and over... So, let's learn how to detect them!

Section 2 begins with a hands-on lab for Kibana, a secondary log aggregation graphical user interface useful for facilitating ransomware and cyber extortion investigations. We then transition from artifact analysis to covering the initial stages of a ransomware campaign attack cycle. We begin by covering Initial Access, Execution, Defense Evasion, and scripting engine abuse. Most ransomware cases involve actors leveraging scripting engines such as PowerShell, Batch scripts, JavaScript, Visual Basic Scripting, and more.

We next discuss the various tools and scripts that we see time and again, providing an overview of each tool along with details for hunting and detection. Next, we move to discussing Persistence. You'll learn about common C2 mechanisms, RMM solutions, and native Windows methods ransomware operators use to maintain access to an environment.

We then pivot to an in-depth review of Cobalt Strike (CS), an adversary emulation and attack simulation tool that has become perhaps "too" good at its job. Many security professionals around the world such as penetration testers and red teams rely on CS. Unfortunately, we see this extremely powerful commercial tool in a very high percentage of ransomware attacks. You will learn about the tool's infrastructure, malleable C2 profiles, payload detection/deobfuscation methods, and more. This module includes a hands-on lab in which you will learn to decode CS payloads.

Much of our training is punctuated with hands-on labs that walk you through analysis methods step-by-step. We aim to ensure that both those with experience and those newer to the realm of incident response can work a ransomware or cyber extortion incident from beginning to end.

TOPICS: Analysis At-Scale via Kibana; Initial Access; Malware infection vs. credential harvesting; Malicious attachments such as MalDocs; Review of our Email Gateway File Block List; Malicious links and how to analyze them; Useful Windows Event Logs; Identifying malicious RDP activity; Zero-day vs. Common Vulnerabilities and Exposures (CVEs); Example CVEs targeted and exploited in the wild; Darknet forum discussions; Execution and Defense Evasion; Free and Open-Source (FOSS); Native scripting engines;l iving Off the Land Binaries and Scripts (LOLBAS); Commercial tooling for adversary emulation; MaaS; PowerShell; Batch scripts; JavaScript scripts; Visual Basic Scripting; Associated Windows Event Logs and enabling them; PowerShell parameters and their purposes; Persistence; Cobalt Strike (CS)

SECTION 3: Advanced Ransomware Concepts

Section 3 begins with Privilege Escalation, Credential Access, and Lateral Movement. What tools do ransomware actors use to escalate privileges on machines? How do they access stored credentials from Windows hosts? What processes are often dumped, why, and how? For lateral movement you'll learn about how RDP, SMB (specifically PsExec), WinRM, and other methods are used to move throughout the victim network.

We then turn our attention to attacks against Microsoft's AD. Ransomware operators love to attack AD, so we'll break down the various ways in which they take advantage of poor AD configurations to escalate privileges and access credentials.

We continue the attack lifecycle with one of the more critical sections of the course – Data Access and Data Exfiltration. Organizations usually want to know what data may have been accessed and/or stolen. We cover data archival and staging methods, including ways to hunt the tools that facilitate these activities. Would you believe that FTP is a common exfiltration route? How can you best detect data being exfiltrated even if you don't know what data is being exfiltrated? We'll show you!

We then move to the final phase of the ransomware attack, Payload deployment and the inner workings of encryption. You'll learn about backup and recovery tampering along with the methods by which ransomware actors attack backup systems. The ways in which actors cover their tracks might seem obvious, because they are! We end this section with technical details pertaining to the most common payload deployment methods.

Finally, we cover hunting methods such as identifying renamed executables, malicious files/processes via directory analysis, common attacks via anti-virus log analysis, and more. This is where we show you the best ways to keep an eye on your organization.

TOPICS: The Phases of a Ransomware Attack Campaign Covered in Section 3: Privilege escalation, Credential access , Lateral movement , Attacks against AD, Data access, Data exfiltration, Payload deployment; Privilege Escalation and Credential Access; Attacks on passwords stored in browsers and password management tools; Session sniffers and extractors; Commonly seen all-in-one solutions (e.g., WinPwn); Lateral Movement; AD Attacks; Data Access; Data Exfiltration; Backup and Recovery; Tampering; Payload Deployment; Hunting Ransomware Operators –Techniques to Identify

SECTION 4: Ransomware Incident Response Challenge

Nothing, and we mean nothing, can better prepare you to respond to ransomware incidents than experience. Since you do not want to gain such experience within your organization, we provide a full day CTF challenge where you will analyze ransomware incidents from the infection vector all the way through the encryption payload running within the environment. We have crafted a victim organization, Samaran Protect, to which you can most likely relate your organization.

Our CTF challenge consists of 50 questions pertaining to a specially crafted attack scenario against our victim organization.

To carry out these attacks, we devised two different ransomware groups, each of which is an amalgamation of currently operating ransomware threat groups. The TTPs leveraged mirror real-world scenarios that those responding to ransomware events see every day. The actors involved in each scenario use different entry methods, credential access methods, tooling, deployment methods, and encryptor payloads.

Furthermore, each scenario mimics a different type of environment: one in which the victim organization does not purposefully collect forensic data to aid in incident response and one in which the victim is well-tooled and is ready for anything. Whether your organization needs to begin all artifact collection and parsing post-incident, or you have augmented your data logging and take advantage of a full-fledged SIEM, the methods we cover in our Capstone will help you relate to your organization's methods and capabilities.

TOPICS: Digital Forensics Capture-the-Flag Event; Review parsed artifact and log data for data collected in Scenario 1; Examine Windows Event logs, Sysmon data, artifacts of program execution, registry hive files, and more; Follow the threat actors' actions from initial infection vector through encryptor payload deployment and execution; dentify the tools, scripts, tactics, and processes used throughout each major phase of each attack campaign; How did the actors get into the network?; What data, if any, were the actors able to access?; Were the actors able to exfiltrate any data?; Which systems were impacted by the overall campaign, including the encryption payload itself?