FOR528: **Ransomware for Incident Responders**

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

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!

Ransomware has become a common occurrence about which we hear in our daily computing lives. The threat of ransomware has evolved over time from being a single machine infection following an ill-advised mouse click to becoming a booming enterprise capable of crippling even large and small networks alike. FOR528 teaches students how to deal with the specifics of ransomware to prepare for, detect, hunt, response to, and deal with the aftermath of ransomware. The class includes multiple hunting methods, a hands-on approach to learning using real-world data, and a full-day, hands-on course capstone to help students solidify their learning.

Ransomware campaigns now follow the Tactics, Techniques, and Procedures (TTPs) of larger-scale, hands-on-the-keyboard attacks. This course shows you what artifacts to collect, how to collect them, how to scale out your collection efforts, how to parse the data, and how to review the parsed results in aggregate. The course also provides in-depth details along with detection methods for each phase of the ransomware attack lifecycle. These phases include Initial Access, Execution, Defense Evasion, Persistence, Privilege Escalation, Credential Access, Lateral Movement, Attacks on Active Directory, Data Access, and Data Exfiltration.

The FOR528 Ransomware for Incident Responders In-Depth Course will help you understand:

- How ransomware has evolved to become a major business
- How human-operated ransomware (HumOR) operators have evolved into well-tuned attack teams
- Who and what verticals are most at risk of becoming a ransomware victim
- How ransomware operators get into their “victim’s” environments
- How best to prepare your organization against the threat of HumOR
- How to identify the tools that HumOR operators often use to get into and perform post-exploitation activities during a ransomware attack
- How to hunt for ransomware operators within your network
- How to respond when ransomware is running actively within your environment
- What steps to take following a ransomware attack
- How to identify data exfiltration

Author Statement

“Ransomware has become ubiquitous. No matter how much we organize to rid the world of the ransomware scourge, we find that ransomware only becomes more common, threat actors become increasingly bold, and organizations continue to buckle under the pressure of these attacks. Luckily for us, the primary methods by which ransomware actors succeed in their attacks involve general failures in “Security 101” practices. If we work together, these can be fixed! Until then, we as security practitioners need to know how to respond to these threats. You and your organization need to know what to collect, how, how to parse that data, and how to analyze that data in a quick and efficient manner. Such is the focus on goal of our course.”
—Ryan Chapman

Section Descriptions

SECTION 1: Ransomware Incident Response Fundamentals

The Ransomware for Incident Responders course begins with a review of ransomeware's history. We begin with the story of the first-known ransomware attack and work our way to the current-day threats that loom above our industry. Our inner-connected lives, not to mention livelihoods, are at risk everyday thanks to the advent of Human Operated Ransomware (HumOR) and Ransomware-as-a-Service (RaaS). You will better your understanding of these threats as we deep-dive into the roles, processes, communication methods, and activities related to these threats. The section then transitions to focus on the Dynamic Approach to Incident Response (DAIR) model and how it relates to ransomware.

After learning about the true threats we face and how we can apply IR 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 and Kibana 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 Virtual Machines; Review of Our Custom Target Victim and their Network; Custom Attack Scenarios Overview; Ransomware Evolution and History; Ransomware-as-a-Service (RaaS); Intrusion Access Brokers (IABs); Ransomware Operators; Forensic Artifact Collection; Incident Response Processes and Their Application to Ransomware; Windows Forensic Artifacts; Analysis at Scale; Analysis GUIs

SECTION 3: Advanced Ransomware Concepts

Day 3 of our course begins with the most feared topics of a ransomware attack: Ransomware 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, simply because they are! We end this section with technical details pertaining to the most common payload deployment methods.

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, and payload detection/deobfuscation methods. This includes a hands-on lab in which you will learn to decode CS payloads.

The next section covers what to do if you are just 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! The days final two sections provide a case study of the Conti ransomware group along with useful hunting techniques. While Conti activity may have recently curtailed, the various leaks we've obtained and analyzed as a community paint a picture of how the group operated. Finally, we cover hunting methods such as identifying renamed executables, malicious files/processes via directory analysis, common attacks via AV log analysis, and more.

TOPICS: Backup and Recovery Tampering; Payload Deployment; Encryption and Decryptors; Cobalt Strike (CS); Dealing with an Active Threat; Ransomware Payments; Conti Case Study; Hunting Ransomware Operators

SECTION 2: Ransomware Modus Operandi

Day two transitions from foundational knowledge 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, and Visual Basic Scripting, and more. In these early sections of the day, we discuss the various tools and scripts that we see time and time 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 Command and Control (C2) mechanisms, Remote Monitoring and Management (RMM) solutions, and native Windows methods ransomware operators use to maintain access to an environment.

We then cover 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 (inc. specifically PsExec), WinRM and other methods are used to move throughout the victim network. Our next section focuses entirely on attacks against Microsoft Acitve Directory (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.

Our final section of the day covers Data Access and Data Exfiltration. This is one of the more critical sections of the course. Organizations always 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? We end the day presenting methods for detecting data exfiltration. How can you best detect data being exfiltrated, even if you don't know what data is being exfiltrated? We'll show you!

TOPICS: Initial Access, Execution and Defense Evasion; Persistence; Privilege Escalation and Credential Access; Commonly targeted accounts; Methods by Which Accounts are Targeted; User Account Control (UAC) Bypass Methods; Local Security Authority Server Service (LSASS) Access and Dumping; NTDS.dit Attacks; Alternate Credentials Attacks; Lateral Movement; Active Directory (AD) Attacks; Data Access; Data Exfiltration

SECTION 4: Course Capstone Challenge

Nothing, and we mean nothing, can prepare you better to respond to ransomware incidents than experience. Since you truly do not want to gain that experience within your organization, we provide a full day Capstone Challenge that will have you analyzing 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 Capstone Challenge consists of over 150 questions pertaining to two specially crafted attack scenarios against our victim organization. Our target victim's network includes 15 hosts with three VLANs

TOPICS: Digital Forensics Capstone; Answer the questions every organization wants answered following a ransomware event, such as:

- How did the actors get into the network?
- What data, if any, were the actors able to access?
- Were the actors able to steal (i.e. exfiltrate) any data?
- Which systems were impacted by the overall campaign, including the encryption payload itself?