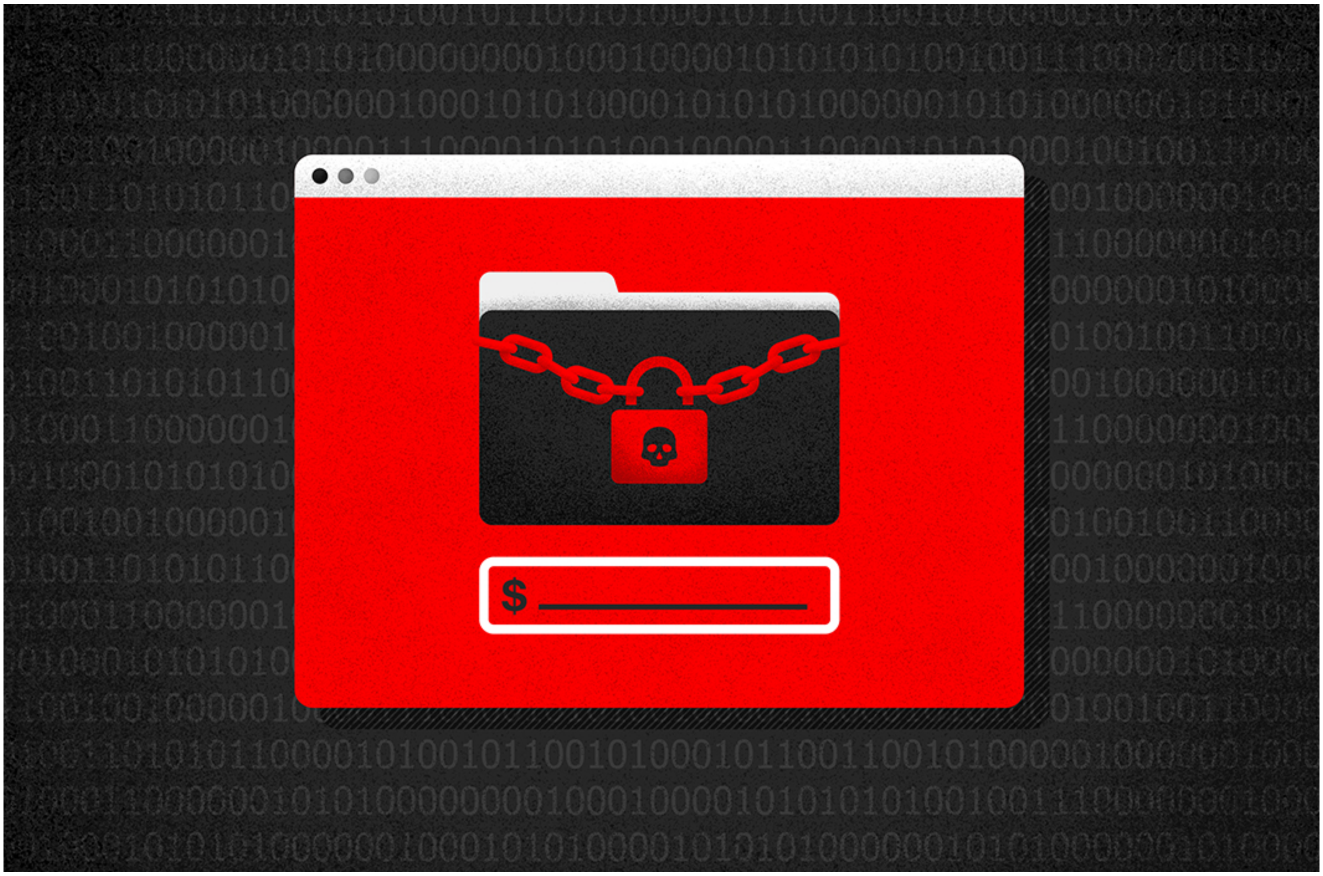
How to Defend Against Conti, DarkSide, REvil and Other Ransomware

crowdstrike.com/blog/how-to-defend-against-conti-darkside-revil-and-other-ransomware/

Josh Dalman - Heather Smith June 2, 2021



CrowdStrike predicted in 2020 that the ransomware threat would only worsen, and news reports since have borne this out. Stories of ransomware attacks since the start of May 2021 alone include:

- *DarkSide* ransomware being used to disrupt a major U.S. pipeline that transports almost half of all fuel consumed on the East Coast of the United States
- The claimed theft of 3 terabytes of sensitive data from part of the Asian operations of a global insurance subsidiary in attacks using *Avaddon* ransomware
- The shutting down of the IT systems of Ireland's Health Service Executive — another victim of a *DarkSide* attack — disrupting patient care throughout the country
- The U.S. Federal Bureau of Investigations (FBI) alerting of a spate of *Conti* ransomware attacks targeting American healthcare organizations and first responder agencies
- The world's largest meatpacking company finding its North America and Australia operations disrupted by a *REvil* ransomware attack thought to have originated in Russia

In addition, not all ransomware attacks make the news, as reflected in CrowdStrike-sponsored research: in a 2020 survey 56% of respondents admitted that their organization had suffered from a ransomware attack in the previous 12 months. Ransomware attacks may go unreported for a variety of reasons, including a desire for confidentiality or a fear of negative business effects for a company.

Ransomware attacks can and do occur in every industry and are increasingly pernicious. The potential financial impact can be staggering. For example, the City of Atlanta estimated that a single ransomware incident in March 2018 cost taxpayers up to $17 million in response and recovery — an estimate that didn't quantify the cost to the community of lost services.

This blog aims to help any organization better prepare its defenses against ransomware attacks and explains how to properly configure your CrowdStrike Falcon® deployment for optimal protection.

Protecting Against Ransomware

The CrowdStrike Services team has written about a number of very effective security controls and practices that you can put in place in your organization to drastically reduce your risk of a ransomware outbreak. Another great source of recommended security controls can be found in SANS CIS Controls version 8. These recommendations can dramatically reduce the risk to your operating environment.

The following recommendations are supported by what the CrowdStrike Falcon Complete™ team has found to successfully prevent and combat ransomware. Additionally, we have included details to assist CrowdStrike customers in making the best decisions for your prevention policies.

Practice Good IT Hygiene

Fundamentally, you can't secure what you can't see. Blind spots, in the form of rogue assets, applications and users, become high-risk attack vectors (and *Conti* ransomware is particularly good at exploiting these weaknesses). Minimizing the attack surface is critical for every organization — it's crucial that you gain visibility into every endpoint and workload running in your environment and then keep any vulnerable attack surfaces updated and protected.

IT hygiene's primary benefit is to give you complete network transparency. This perspective provides a bird's eye view, as well as the power to drill down and proactively clean out your environment. Once you achieve this level of transparency, the understanding of "who, what and where" that IT hygiene provides has tremendous benefits for your organization. You're able to:

- **Identify gaps in your security architecture.** The clarity that IT hygiene provides allows you to see what hosts are running on your environment and whether they are protected. Having complete visibility enables you to effectively deploy your security architecture and ensure no rogue systems are operating behind your walls. The larger and more distributed your environment becomes — such as with workforces going increasingly remote — the harder it is to have visibility across all of your endpoints and identities (including both human and service accounts). Identifying the unmanaged assets in your environment allows you to target vulnerabilities and protect your valuable assets before attackers can reach them.
- **See what is running in your environment.** By proactively identifying outdated and unpatched applications and operating systems, you can manage your application inventory and solve security and cost problems simultaneously. Unpatched operating systems and applications have serious security and cost implications — make sure to identify which applications are running on your network and pinpoint unpatched apps to get ahead of attackers.
- **See who is running in your environment.** Account monitoring allows you to see who is working in your environment and ensure they're not violating their credential permissions (including detection of tools or behavior trying to subvert those policies). System administrators remain highly targeted, and combined with poor password renewal policies, credential theft is a harsh reality. With insight into password updates, you can prevent credential creep by removing old administrative accounts or making sure users update their passwords regularly. Taking this a step further, visibility into unusual admin behavior or privilege elevation can prevent silent failure by tipping off your security team as soon as something suspicious occurs.
- **Ensure user compliance.** Making sure your users abide by your most up-to-date password policies keeps administrators and users compliant with your security requirements. Consistent and ongoing user education can ensure that password best practices are followed, and ridding your network of old accounts (including service accounts) can mitigate the risk of "credential creep" by former employees.
- **Add defense-in-depth.** Implement real-time detection policies to monitor for anomalous credential behavior use, including detection of lateral movement even on workstations that may not have a Falcon agent installed. In addition, enable risk-based conditional access to trigger MFA for human and service accounts without adding burden to users, ensuring higher compliance.

Once you have full visibility and understanding of your environment, your organization can identify hygiene-related security deficiencies and resolve them immediately. From there, security teams can quickly pivot to address the critical elements of comprehensive endpoint protection: prevention, detection, hunting and threat intelligence. These capabilities are key to a complete solution that can protect your organization from the most motivated, sophisticated attackers. With a "hygiene-first" approach, and the right security solution in place, you can protect your organization from ransomware attacks and stop breaches.

In addition to the general best practices outlined above, the following are specific IT hygiene steps to take to protect against ransomware in particular:

- **Do not allow hosts on the internet with exposed RDP port 3389.** If you must have RDP internet-facing for business productivity purposes, there are many compensating controls you will want to consider (see the 2FA/MFA recommendation below).
- **Disable host-to-host communications as strictly as possible.** Commonly, lateral movement occurs via authenticated SMB connections. Remote service creation allows for an attacker to create a service on a remote host, then they can drop a binary into the path where they've told the service to point to. This is a very common malware lateral movement technique that is also highly associated with ransomware of late. Enable behavioral detection controls to flag anomalous activity such as service account usage from workstation to workstation (and block service account usage for any interactive login, such as RDP). In addition, enable key adversary tool detection use (like Mimikatz) through identity-centric protocol analysis.
- **Consider all administrative activities to occur via a jump host (and enable identity policy to force administrative use via jump host only).** Your host-based firewall (or Falcon Firewall Management™) can be configured to allow SMB, remote PowerShell, etc., from your jump host IP address. This jump host should be the source for your administrative activity or changes. Adversaries will know this and may target that host, so we'll point you back to SANS CIS Controls and recommend that you do not skip a beat on your jump host.
- **Apply two-factor authentication (2FA)/multifactor authentication (MFA).** 2FA and MFA are typically at the top of recommended security controls, but we regularly see adversaries accessing networks via single-factor VPN authentication as well as single-factor internet-exposed RDP. Prioritizing MFA everywhere is critical to this conversation. To ensure use of MFA everywhere, also consider enabling conditional access policies that trigger based on key conditions and risk factors to reduce the burden of MFA and thus wider adoption.

Configure the Falcon Platform Properly

Use Proper Prevention Policy Settings. In many organizations, security personnel must balance the needs and productivity tolerances of the business with the implementation of security controls. The Falcon Complete team recommends enabling most, if not all, of the configurations within the Falcon platform's Prevention Policy Settings, yet we realize this won't happen for every asset at every organization. For example, some organizations have assets where any disruption whatsoever could lead to thousands of dollars of revenue loss every second. It's common for the demands of productivity to require prevention policy settings to be dialed back. It's also common for attackers to find the dark corners of the network and conduct their attacks on, or from, these types of systems.

(CrowdStrike customers who would like additional information about the specific prevention policy settings recommended by the Falcon Complete team can log in here.)

Keep Up With Sensor Updates. One common miscalculation the Falcon Complete team observes organizations make is to continue to do sensor updates manually through their existing solution such as SCCM. If you have a top-notch patching program and can achieve sensor updates when they're made available to the Falcon platform, by all means, continue achieving success in this area.

The cloud-delivered Falcon platform enables the ability to quickly toggle sensor versions to various host groups. Falcon Complete recommends utilizing the N-1 methodology to update all systems aside from a test group where you test the latest sensor when it becomes available within the platform. This configuration updates the sensor to the version released immediately prior to the latest release. This allows all CrowdStrike customers to test the sensor for bugs, and also for you to test with a sampling of systems within your network. CrowdStrike is consistently updating detections, machine-learning models and functionality in our sensor. Going months without an update can leave your environment unprotected from the latest trends that security engineers are tooling detections for.

Deploy the Falcon Agent 100%. The number one reason Falcon Complete customers become compromised is not having the agent deployed to all compatible assets. We see lateral movement alerts nearly every day from that dark corner of customer networks, even when an agent cannot be installed on the endpoint. The Falcon Discover™ module has a dashboard that can help identify "Unmanaged Assets." Again, this piece is fundamentally critical to the ransomware conversation. Spend the time to dig into the appropriate reports and track down assets that do not have the Falcon agent on them.

When it is not possible to place an agent on all assets, having a CrowdStrike Falcon Identity Protection solution to detect and enforce policy can stop lateral movement, detect anomalous use of service accounts (e.g., interactive logins as seen with RDP), and detect the use of certain tools such as Mimikatz that are commonly used in ransomware attacks.

Know When to Ask for Help

In the event that you believe your organization may be impacted by ransomware, calling in experts to help investigate, understand and improve the situation can make the difference between a minor incident and a major breach. In some instances, organizations become aware of threat actor activity within their environment but may lack the visibility to address the problem or the right intelligence to understand the nature of the threat. Getting educated about the latest threats and seeking help by activating an incident response team or retainer, such as those offered by CrowdStrike Services, may allow for detection and remediation before the threat actor is able to deploy ransomware or exfiltrate data from the environment.

It’s better yet to seek out expert assistance before you truly need it. A technical assessment can help you to proactively identify and understand factors about your organization’s network that could make future ransomware incidents more or less likely. It may take different forms, depending on your current needs and security maturity. For instance, if you experience an intrusion that was confined to a specific network segment or specific business unit, an enterprise-wide compromise assessment can give confidence that the attacker did not move into parts of the environment that were beyond the scope of the initial investigation. Alternatively, an IT hygiene assessment can identify weak passwords, Active Directory configurations or missed patches that could open the door to the next attacker.

Additional Resources

- *Read about recent intrusion trends, adversary tactics and highlights of notable intrusions in the CrowdStrike 2021 Global Threat Report.*
- *Understand the trends and themes that we observed while responding to and remediating incidents around the globe in 2020 — download the latest CrowdStrike Services Cyber Front Lines Report.*
- *Learn more about Falcon Complete by visiting the product webpage.*
- *Find out more about the CrowdStrike Falcon® platform by visiting the product webpage.*
- *Test CrowdStrike next-gen AV for yourself. Start your free trial of Falcon Prevent™ today.*