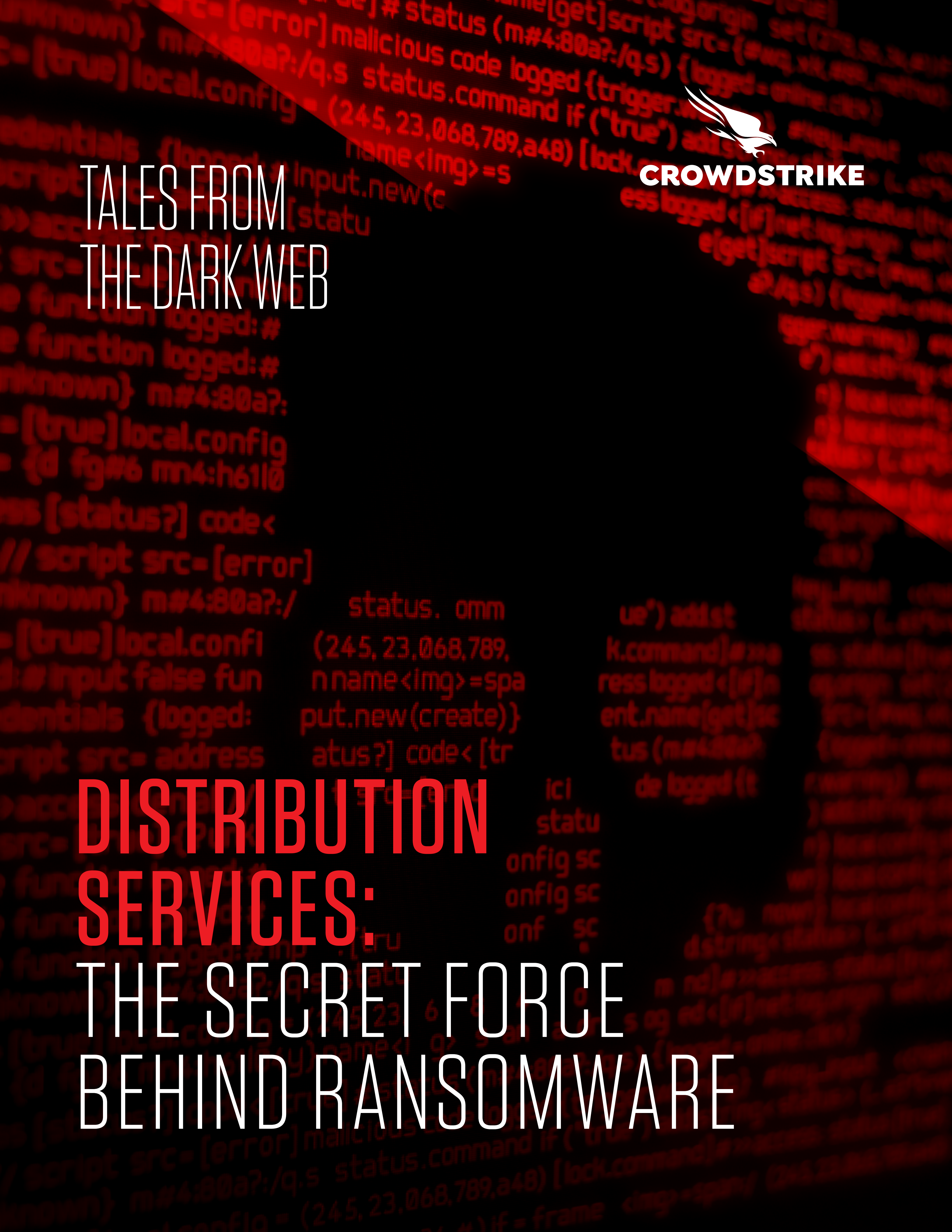


CROWDSTRIKE

TALES FROM
THE DARK WEB

DISTRIBUTION SERVICES: THE SECRET FORCE BEHIND RANSOMWARE

ABSTRACT

Ransom and extortion have been around for decades. Yet 2021 was one of the most active years for ransomware operators targeting organizations of all sizes worldwide. In this white paper we explore how ransomware actors continuously grow their victim list and maximize ransom payouts by actively recruiting affiliates to help them distribute their malicious payloads. We also review how defenders can leverage many types of front-line threat intelligence to understand the complex sequence of ransomware enablers and help obtain critical insights to stop adversaries in their tracks.

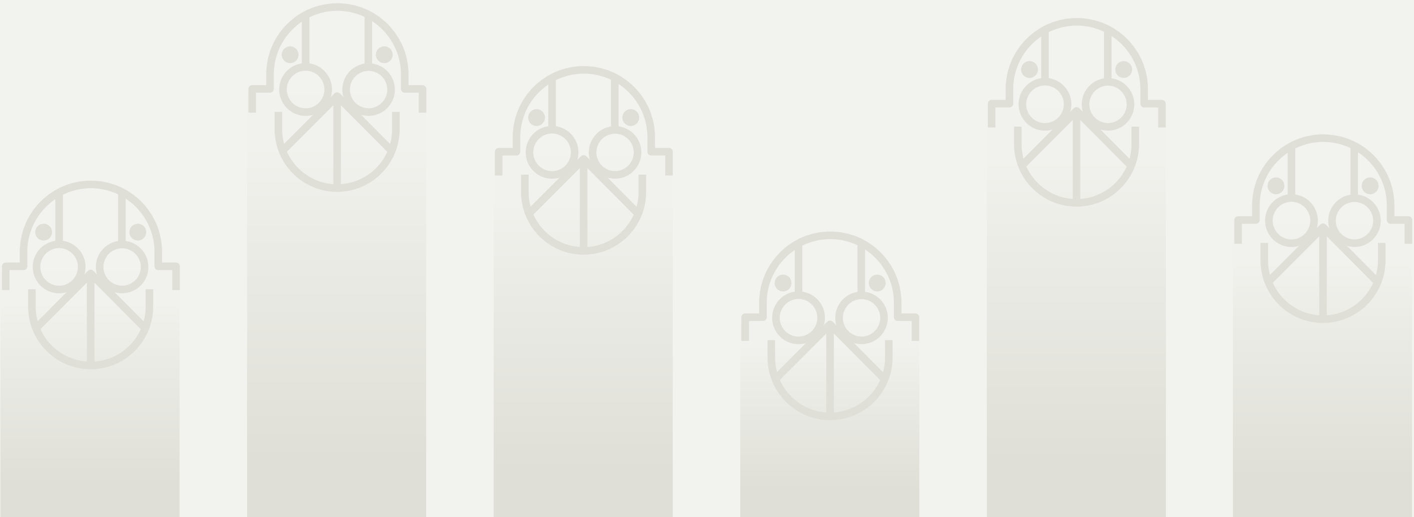
THE RISE OF RANSOMWARE

Over the past two years, the number of ransomware incidents and payouts has grown substantially.

According to the **2021 CrowdStrike Global Security Attitude Survey**, 66% of respondents' organizations suffered at least one ransomware attack in the prior 12 months. The average ransom payment increased by 63% in 2021 to $1.79 million USD compared to 2020, and a whopping 96% of organizations that paid a ransom reported being hit with additional extortion fees, costing them on average $792,493 USD. These numbers of course cover the publicly known payouts; according to CrowdStrike **eCrime Index** data, the actual demand ransom surpassed this number by three times.

Other sources also confirm this trend. The FBI's Internet Crime Complaint Center (IC3), which provides the public with a trustworthy source for reporting information on cyber incidents, received 2,084 ransomware complaints from January to July 31, 2021, a 62% increase compared to the same timeframe in 2020 (**https://us-cert.cisa.gov/ncas/alerts/aa21-243a**).

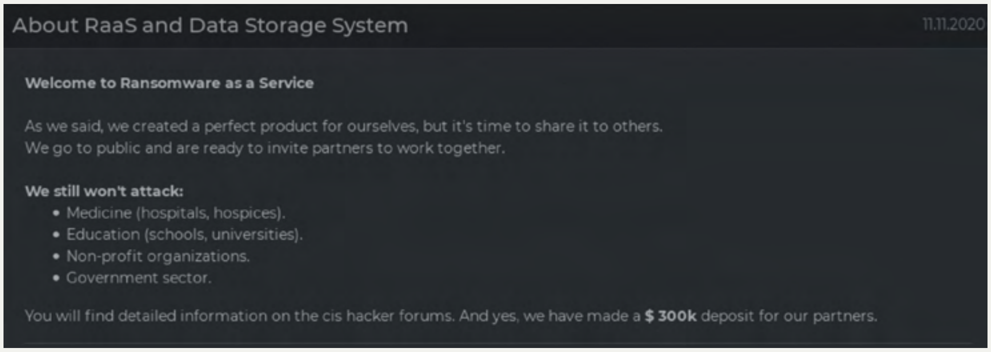
These numbers are sobering and beg the questions: **"Who are the core actors behind this jump in ransomware?"** and more importantly, **"How do they continuously expand their victim list?"**



THE LUCRATIVE BUSINESS MODEL OF RANSOMWARE OPERATORS AND AFFILIATES

When reviewing recent ransomware campaigns like *REvil*, *Conti* or *DarkSide* in detail, it is clear that the operators behind these offensive programs don't work in isolation. CrowdStrike Intelligence has discovered actors like CARBON SPIDER and PINCHY SPIDER announcing themselves on thriving criminal communities to recruit affiliates interested in helping them spread their ransomware and share profits. These affiliates join from a broad international theater and often specialize in identifying eCrime targets. In return for helping to distribute the disruptive malware, the recruiting operator will support the affiliate in several ways, including:

- Providing training or playbooks on how to move laterally
- Packaging customized ransomware so affiliates can distribute the malware over their own channels and combine with other attack tools
- Providing internet infrastructure for data exfiltration and storage
- Providing built-in covert communication channels to obfuscate or hide the affiliate during conversations with the victim
- Sharing detailed payment instructions to receive cryptocurrencies from victims
- Providing professionalized public or media-promoted outlets (e.g., dedicated leak sites, aka DLSs) to extort victims post-compromise and maximize payments


About RaaS and Data Storage System

11.11.2020

Welcome to Ransomware as a Service

As we said, we created a perfect product for ourselves, but it's time to share it to others.
We go to public and are ready to invite partners to work together.

We still won't attack:

- Medicine (hospitals, hospices).
- Education (schools, universities).
- Non-profit organizations.
- Government sector.

You will find detailed information on the cis hacker forums. And yes, we have made a **$ 300k** deposit for our partners.

Figure 1. DarkSide DLS ransomware-as-a-service announcement

On the other hand, affiliates — with assistance from access brokers — specialize in carefully identifying victims by scanning victim infrastructure or architecting social engineering assaults to undermine user confidence and gain initial access. Victims are often selected based on revenue and their likelihood of available funds to pay a ransom. Based on their research, affiliates also often set ransom payouts to maximize profits.

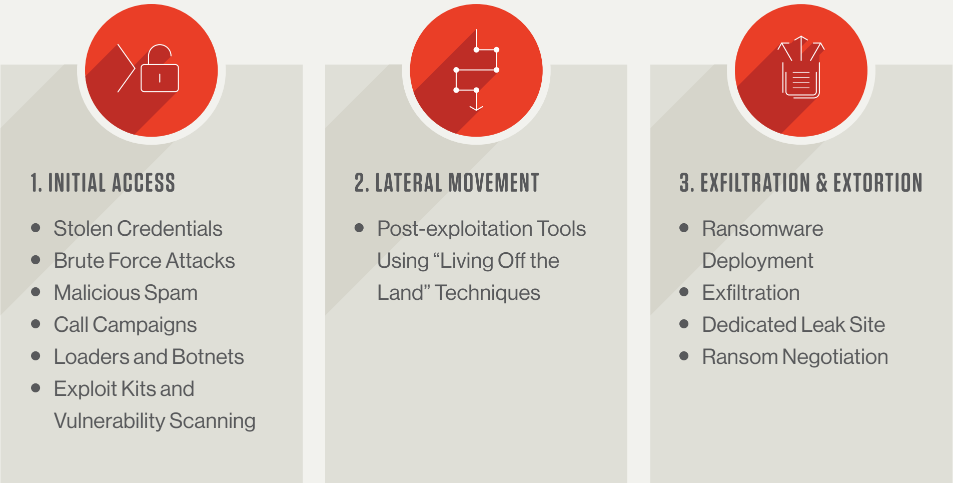
This lucrative business model between ransomware operators and affiliates creates a perfect storm for victims, as affiliates do not need any expertise on how to build malicious content, and the likelihood of operating with impunity is very high. Because affiliates carefully choose their victims and use optimized delivery methods, ransomware campaigns like *REvil* and *Conti* often stay afloat for many months while ransomware operators rake in payments.

Ransomware-as-a-Service (RaaS): Dynamics Between Ransomware Operators and Affiliates

RaaS Operator	Affiliate
■ Recruits affiliates on forums	■ Pays to use the ransomware ■ Agrees on a service fee per collected ransom
■ Gives affiliates access to a "build your own ransomware package" panel ■ Creates a dedicated "Command and Control" dashboard for the affiliate to track the package	■ Targets victims ■ Sets ransom demands ■ Configures post-compromise user messages
	■ Compromises the victim's assets ■ Maximizes the infection using "living off the land" techniques ■ Executes ransomware
■ Sets up a victim payment portal ■ "Assists" affiliates with victim negotiations	■ Communicates with the victim via chat portals or other communication channels
■ Manages a dedicated leak site	■ Manages decryption keys

DISTRIBUTION SERVICES TO DEPLOY THE RANSOMWARE

Based on technical and incident insights from several ransomware campaigns like *REvil*, *Conti* and *DarkSide*, CrowdStrike Intelligence analysts discovered multiple initial access and lateral movement techniques used by affiliates prior to deploying the ransomware and maximizing the effect on the victim. By continuously changing the mix of these enablers or distribution services, actors create novel ways to bypass security measures.



1. INITIAL ACCESS

- Stolen Credentials
- Brute Force Attacks
- Malicious Spam
- Call Campaigns
- Loaders and Botnets
- Exploit Kits and Vulnerability Scanning

2. LATERAL MOVEMENT

- Post-exploitation Tools Using "Living Off the Land" Techniques

3. EXFILTRATION & EXTORTION

- Ransomware Deployment
- Exfiltration
- Dedicated Leak Site
- Ransom Negotiation

Figure 2. Stages of a ransomware attack, including techniques

Let's take a look at different examples of distribution services that provide the adversary with initial access.

INITIAL ACCESS USING STOLEN CREDENTIALS ACQUIRED FROM ACCESS BROKERS

Affiliates often use leaked credentials to gain initial access. Remote Desktop Protocol (RDP) is a popular starting point as it offers a direct view to a victim's asset and is a great stepping stone for lateral movement.

In 2020, CrowdStrike Intelligence threat researchers discovered an active underground marketplace offering the sale of compromised RDP credentials advertised on multiple Russian-language underground forums. Although the majority of the RDP offerings in the shop are residential, corporate RDPs are available upon request.

Anyone with cryptocurrency and a user account for one of these RDP shops can purchase and use the compromised RDP account for malicious purposes. Once remote access is established, it allows users to start escalating privileges and stealing more credentials.

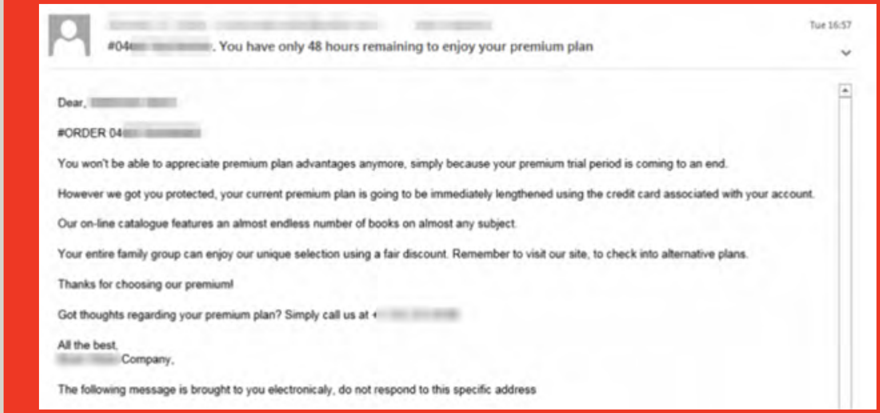
SPAM OR SOCIAL ENGINEERING CAMPAIGN

Spam in combination with socially engineered targets remains one of the most popular vectors to distribute malware. While email is an important mechanism to initially communicate with the victim, it is no longer the only mechanism. At the end of April 2021, the CrowdStrike Intelligence team discovered usage of "fake" call centers and even search engine manipulation to trick users into downloading and installing malicious documents (see the "Malcall" campaign example below).

Example "Malcall" Campaign

WIZARD SPIDER, an established, high-profile and sophisticated Russia-based eCrime group, evolved over the past 5 years into a highly capable group with a diverse and potent arsenal. Their toolset covers the entirety of the kill chain, from delivery to post-exploitation tools and big game hunting (BGH) ransomware, enabling them to conduct a wide range of criminal activities against enterprise environments.

In April 2021, CrowdStrike Intelligence observed **WIZARD SPIDER** conducting an account-themed spam campaign to deliver their proprietary malware *BazarLoader*. The technique involves a social engineering lure referencing a subscription expiration date and the automatic renewal of a "premium plan" (see Figure 3 below). Victims are enticed into calling a U.S.-based phone number to dispute the subscription renewal and are subsequently led through a process, supposedly to cancel the subscription, that ultimately leads to the deployment of *BazarLoader* via malicious, macro-enabled Microsoft Office documents (typically Excel spreadsheets).



[redacted]

Tue 16:57

#04[redacted]. You have only 48 hours remaining to enjoy your premium plan

Dear, [redacted]

#ORDER 04[redacted]

You won't be able to appreciate premium plan advantages anymore, simply because your premium trial period is coming to an end.

However we got you protected, your current premium plan is going to be immediately lengthened using the credit card associated with your account.

Our on-line catalogue features an almost endless number of books on almost any subject.

Your entire family group can enjoy our unique selection using a fair discount. Remember to visit our site, to check into alternative plans.

Thanks for choosing our premium!

Got thoughts regarding your premium plan? Simply call us at [redacted]

All the best,
[redacted] Company,

The following message is brought to you electronicaly, do not respond to this specific address

Figure 3. *BazarCall* phishing email

The infection chain consists of the following stages:

1. The victim receives the *BazarCall* email.
2. The victim contacts the phone number and requests a cancellation.
3. A call center operator directs the user to a fake website to complete the cancellation process.
4. The victim is socially engineered into downloading an MS Office document containing malicious macros.
5. The victim is instructed to open the document and enable editing and content, which executes the malicious macros and installs *BazarLoader*.

VULNERABILITY SCANNING AND EXPLOIT KITS

Exploit kits can be found on multiple forums. They target specific software or systems to install additional code and obtain access. Exploit kits can also be combined with phishing campaigns to maximize their effects.

An older popular example is the RIG exploit kit that can be distributed through malvertising or malicious campaigns and uses Adobe Flash exploits based on CVE-2018-8174 to inject itself into a target's machine, after which it deploys a payload such as a loader, botnet or information stealer.

More recently, in August 2021, CrowdStrike internal and public sources reported an increase in malicious activity associated with the ProxyShell exploit chain. ProxyShell refers to a sequence of vulnerabilities that can be exploited to achieve remote code execution (RCE) on unpatched Microsoft Exchange Servers.

ECrime actors shifted to exploitation of exposed Microsoft Exchange Servers throughout 2020 and 2021. The inherent exposure and extended patching cycles associated with Exchange servers previously resulted in prolonged exploitation of CVE-2020-0688. The CrowdStrike Intelligence team foresees that eCrime actors will continue to exploit Exchange servers vulnerable to ProxyShell in the near term.

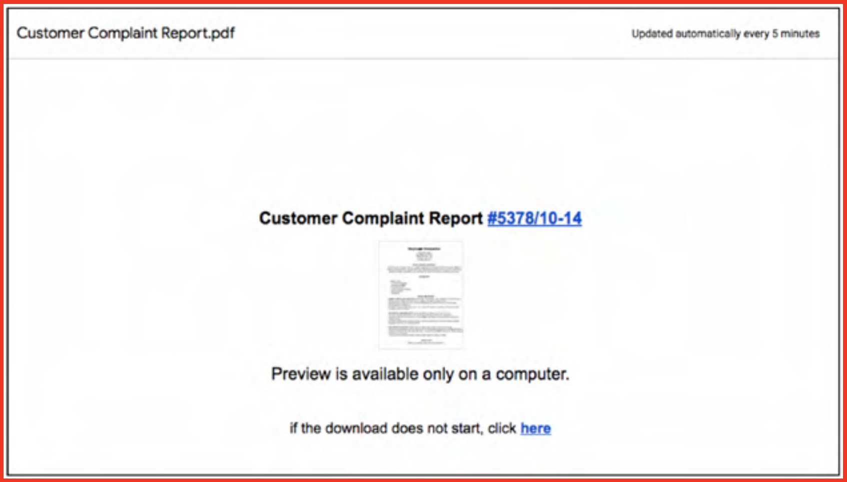
LOADER AND BOTNET USAGE

Loaders are often an intermediary step between phishing campaigns and ransomware deployment. They leverage malicious documents like macro-enabled spreadsheets that will download and execute malicious code. Once compromised with the loader or botnet, the victim's client is ready for additional malware or a remote access tool (RAT).

Sample Loader: WIZARD SPIDER use of *BazarLoader*

WIZARD SPIDER, is originally known for the creation and operation of the *TrickBot* banking malware for the purpose of conducting financial fraud. After a takedown attempt on *TrickBot* in September 2020, CrowdStrike Intelligence observed increased use of *BazarLoader*. This loader has been distributed in spam operations and used as an additional infection vector leading to initial access.

The identified *BazarLoader* spam runs consist of emails containing a link to a Google Docs file (Figure 4). The Google Docs file commonly contains a link to the *BazarLoader* payload hosted on an external site.



Customer Complaint Report.pdf

Updated automatically every 5 minutes

Customer Complaint Report #5378/10-14

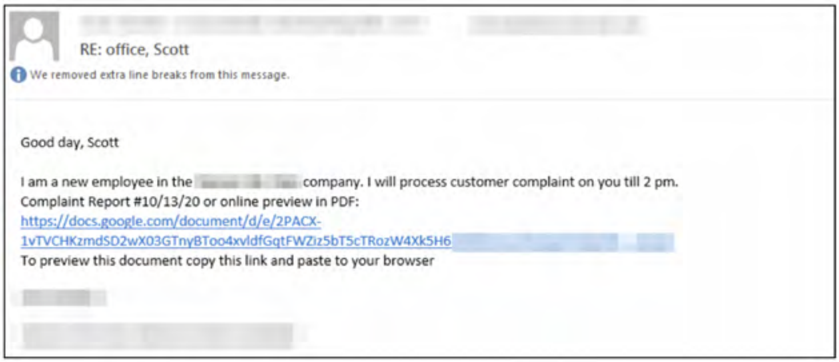
Preview is available only on a computer.

if the download does not start, click here

Figure 4. Example *BazarLoader* Google Docs File

Sample Loader: WIZARD SPIDER use of *BazarLoader*

The spam emails are often business-related, with themes that reference purported phone calls, meetings, customer complaints or employment termination. An example email is provided in Figure 5.



[redacted]

RE: office, Scott

We removed extra line breaks from this message.

Good day, Scott

I am a new employee in the [redacted] company. I will process customer complaint on you till 2 pm.
Complaint Report #10/13/20 or online preview in PDF:
https://docs.google.com/document/d/e/2PACX-1vTVCHKzmdSD2wX03GTnyBToo4xvldfGqtFWZiz5bT5cTRozW4Xk5H6[redacted]
To preview this document copy this link and paste to your browser

[redacted]

Figure 5. *BazarLoader* Spam Email with Google Docs Link

BazarLoader (aka *Kegtap*) consists of a loader and a backdoor component.

- **The loader** is responsible for installing and executing the backdoor element. The discovered version of the loader contains a large amount of string and code obfuscation, and it has been observed utilizing a novel technique of mimicking legitimate software for persistence. CrowdStrike technical analysis has specifically revealed the loader mimicking communications software such as Softphone.
- **The backdoor** component is capable of executing arbitrary payloads, batch and PowerShell scripts, exfiltrating files from a victim, and terminating running processes. In addition to the backdoor component, Crowdstrike observed WIZARD SPIDER deploying and utilizing the Cobalt Strike post-exploitation framework.

POST-EXPLOITATION TOOLS AND "LIVING OFF THE LAND" FOR LATERAL MOVEMENT

Once access is gained to a system, adversaries will continue to explore the network to find critical data or applications, maximizing the effect on the victim's infrastructure. To go undetected, these threat actors will leverage built-in system tools like PSExec, PowerShell scripts or WMI (Windows Management Instrumentation) to execute tasks and go unseen. These methods are often referred to as "living off the land."

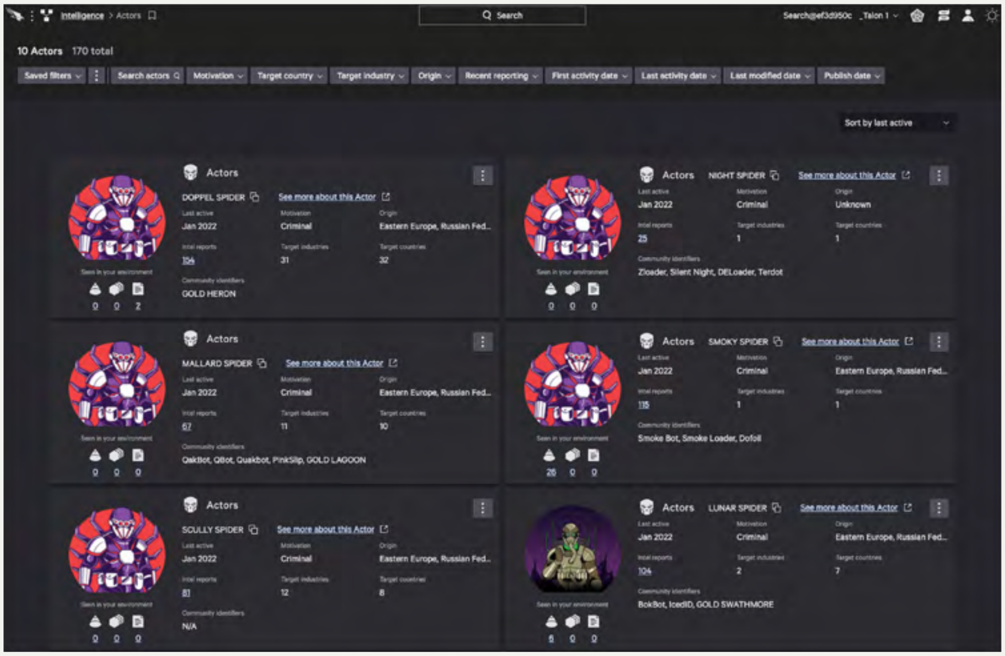
A common popular tool has been **Cobalt Strike**, a commercial, full-featured remote access tool that bills itself as "adversary simulation software designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors." Cobalt Strike's interactive post-exploit capabilities cover the full range of attack tactics, all executed within a single, integrated system. It is the premier choice for actors conducting post-exploitation activities.

The CrowdStrike Falcon OverWatch™ threat hunting team detected threat actor **SPRITE SPIDER** at a North America-based food and beverage company. The adversary used cmd.exe to run a PowerShell command to execute a remote file on two hosts. SPRITE SPIDER has previously used AWS elastic compute cloud (EC2) domains to host Cobalt Strike command-and-control servers.

THE DEFENDER'S VIEW: AVOIDING THE PERFECT STORM

For defenders, a cascading sequence of distribution services generates a layer of complexity. Distribution tools are known to evade detection, may be short-lived and can even come with built-in anti-forensics. Defenders need to rely on external threat intelligence to understand prevalent adversarial techniques in advance in order to scale up detection and prevention. The following are some core insights that any organization needs in order to fight distribution services delivering ransomware.

The adversary universe: Behind every attack is an adversary with motivations and techniques. The list and activities of bad actors change continually. Defenders must understand which criminal actors are actively recruiting affiliates, who they are targeting and how they operate. By focusing on the adversary universe targeting their environment and understanding their tools of trade, defenders can execute an intelligence-first defense strategy and plan resources based on threat facts.



10 Actors 170 total

Actors	Last active	Motivation	Origin	Intel reports	Target industries	Target countries	Community identifiers	Seen in your environment
DOPPEL SPIDER	Jan 2022	Criminal	Eastern Europe, Russian Fed...	104	31	32	GOLD HERON	0 0 2
NIGHT SPIDER	Jan 2022	Criminal	Unknown	25	1	1	Zloader, Silent Night, DELoader, Terdot	0 0 0
MALLARD SPIDER	Jan 2022	Criminal	Eastern Europe, Russian Fed...	67	11	10	QakBot, QBot, Quakbot, PinkSlip, GOLD LAGOON	0 0 0
SMOKY SPIDER	Jan 2022	Criminal	Eastern Europe, Russian Fed...	115	1	1	Smoke Bot, Smoke Loader, Dofoil	26 0 0
SCULLY SPIDER	Jan 2022	Criminal	Eastern Europe, Russian Fed...	81	12	8	N/A	0 0 0
LUNAR SPIDER	Jan 2022	Criminal	Eastern Europe, Russian Fed...	104	2	7	BokBot, IcedID, GOLD SWATHMORE	6 0 0

Figure 3. CrowdStrike Falcon X actor portal provides details about threat actors, including motivation, targets and kill chain

Attack methods, indicators of compromise (IOCs) and exploits: Ransomware campaigns come and go. After a period of activity, they usually go silent for a short time to retool and reorganize. For defenders, knowing which ransomware campaigns and related distribution tools are active versus which ones are going into sleep mode is crucial. By understanding the tactics, techniques and procedures (TTPs) surrounding the distribution campaigns, security teams can react via improved detection by downloading machine-readable indicators (e.g., IOCs, Snort, YARA rules) and even prevent imminent attacks by reducing attack surfaces vulnerable to exploits. In addition to reactive detection, security planners can adjust proactively controls by consuming intelligence reports like threat alerts, malware technical analysis (also called tippers) and global threat trends describing emerging adversarial attack behaviors.

Monitoring criminal underground forums: Credentials or bots are often put up for sale on various underground forums. Defenders can be alerted to criminal posts targeting their organization's critical assets. These alerts can help victims identify a threat prior to the ransomware deployment so they can investigate and remediate faster.

Investigating malicious files: Ransomware operators and distribution services often reuse existing attack tools. When malicious files are discovered, cyber threat intelligence teams need to be able to find related malware samples to understand file behavior, attributes, malware family and adversary attribution. Using this information, effective remediation and recovery steps can be executed so attackers remain locked out.

DECISION MAKING WITH FRONT-LINE INTELLIGENCE

The dangerous cocktail of ransomware operators and affiliates that are recruited on criminal forums creates a formidable, fast-growing opponent for cybersecurity teams. The toxic mix of stealthy and quickly changing distribution services, prior to the distribution of ransomware, makes protection, detection and remediation of these fast-growing attacks a challenge.

To fight this complexity, defenders need a full scope of threat intelligence insights starting from the eCrime universe, underground forums, the actors, motivations down to the tools, techniques and procedures surrounding the attack campaigns all delivered timely to prepare and stop these lucrative adversaries in their tracks.

ABOUT CROWDSTRIKE

CrowdStrike Holdings, Inc. (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with one of the world's most advanced cloud-native platforms for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: **We stop breaches.**

Request a Free Intelligence Briefing

Learn more about CrowdStrike Threat Intelligence offerings

©2022 CrowdStrike, Inc. All rights reserved.