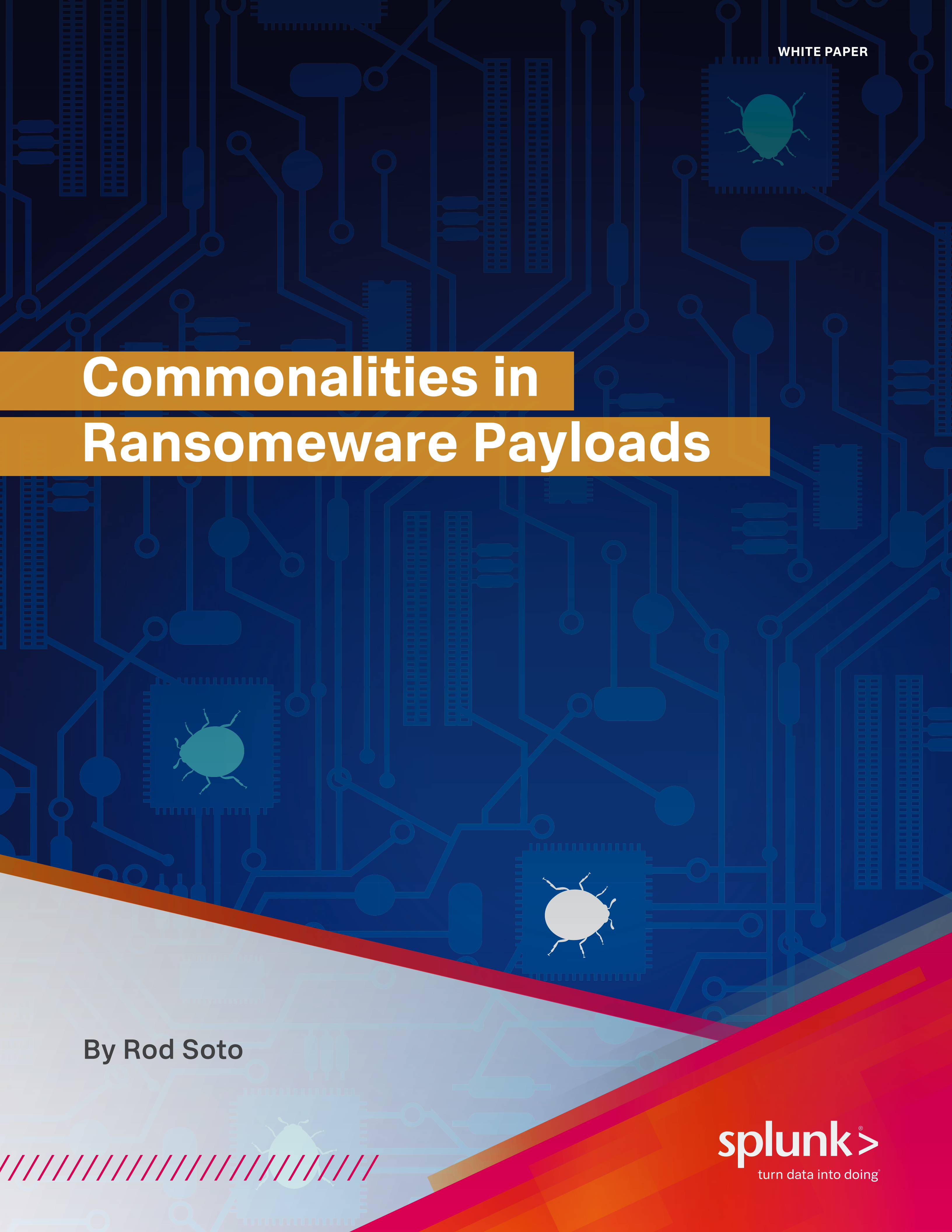
WHITE PAPER

Commonalities in Ransomeware Payloads

By Rod Soto



splunk>
turn data into doing

Over the last year, we've seen a significant increase in malicious attacks involving ransomware payloads. According to the Federal Bureau of Investigation (FBI), as many as 2,048 ransomware complaints were registered in 2021. The Financial Crimes Enforcement Network also reported 68 variants of ransomware, accounting for over $590 million in ransom payments.

These types of threat campaigns continue to reach millions of Americans every day — increasing gas prices, disrupting healthcare, utilities, government and education, as well as impacting a long list of other sectors. Ransomware has become a threat to national security, which invited a response from the Whitehouse including sanctions, law enforcement coordination, and directives to US Cyber Command (USCYBERCOM) and the National Security Agency (NSA) to act against the groups responsible.

The Splunk Threat Research Team (STRT) addresses several well-known ransomware payloads. As the team researched these variants, a number of important insights were collected, including specific payload signatures, techniques and procedures associated with each of these malicious threat groups. STRT's research was also able to discover several commonalities between these ransomware payloads. This white paper outlines these findings, with a special focus on what we consider common attack categories for destructive payloads — regardless of variant or platform.

Ransomware Payloads: Analytic Stories From 2020-2021

Ryuk

December 2020

Malicious campaign targeting healthcare and the public healthcare sector. (Reference.)

Clop

December 2020-April 2021

Malicious campaign targeting several verticals. Largest ransom payment to date at $20 million. (Reference.)

Darkside

March-May 2021

Ransomware attacks against U.S. utility organizations. Colonial pipeline is compromised and operations are suspended temporarily. (Reference.)

Conti

July 2021

Malicious campaign against healthcare and first responder networks. (Reference.)

Blackmatter

July 2021

Malicious campaign against multiple U.S. based organizations with possible links to the Darkside group. (Reference.)

REvil

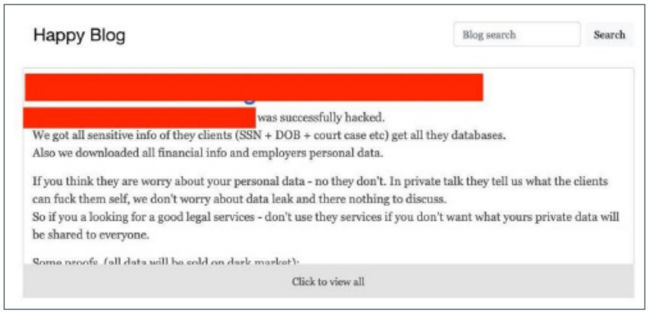
June-December 2021

Malicious campaigns executed against supply chain management vendors across several verticals (MSP, SAAS, PAAS). (Reference.)

What is the goal of ransomware and how effective is it?

Thanks to these campaigns, threat groups have amassed a large fortune via ransomware. Their motive is usually financial profit — and these profits usually far outweigh any time or effort invested into said campaigns. In plain terms, ransomware is a great business to be in if you're a cybercriminal. In 2021 alone, over 590 million dollars was successfully swindled via ransomware.

Ransomware payloads are fundamentally destructive. Even if the victim pays full ransom, the recovery of the victim's data isn't guaranteed — and highly unlikely. Worse yet, many of these campaigns employ what's called a "double extortion scheme." This is when malicious actors exfiltrate data in addition to encrypting user and system files. These groups then attempt to sell the victim's data on the dark web. This includes proprietary data, credit card details, social security numbers, log-in credentials, personal pictures, identity documents, trade secrets and more.



Happy Blog

Blog search | Search

[redacted]

[redacted] was successfully hacked.
We got all sensitive info of they clients (SSN + DOB + court case etc) get all they databases.
Also we downloaded all financial info and employers personal data.

If you think they are worry about your personal data - no they don't. In private talk they tell us what the clients can fuck them self, we don't worry about data leak and there nothing to discuss.
So if you a looking for a good legal services - don't use they services if you don't want what yours private data will be shared to everyone.

Some proofs (all data will be sold on dark market):

Click to view all

Source: Zdnet

Ultimately, these groups profit from selling sensitive information and collecting ransom from their victims — making ransomware an incredibly lucrative business for cybercriminals.

Criminal Gangs
Operate with near impunity

Industry Sectors
Unprepared, neglectful, careless

Unregulated Cryptocurrencies
No KYC, AML

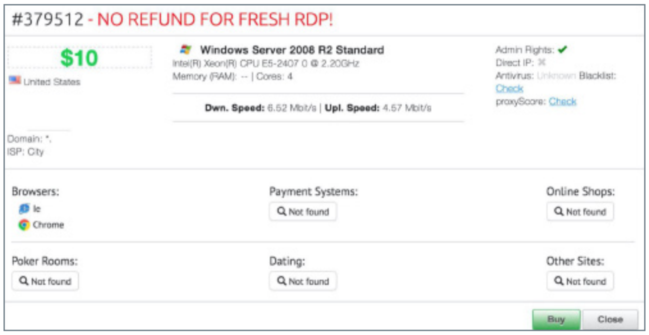
First and foremost, criminal groups often operate with near impunity. Public entities (e.g., foreign government bodies, geopolitical adversaries) may look the other way, claiming extraterritoriality in order to avoid responsibility for these types of advanced persistent threats (APTs). However, the truth is that these groups are often state-sponsored, possessing strategic value and sensitive intel to their benefit.

With certain threat groups leading the charge, nation-states can claim plausible deniability if anything comes under scrutiny, allowing them to skirt international sanctions according to the Ransomware Task Force. This is facilitated by the use of cryptocurrencies, which are mostly unregulated, very hard to monitor and track, and unlimited in their ways of sending, mixing and creating obfuscated means to hide the destinations of these ransom payments.

Finally, many of the victims have weak (or nonexistent) security, leading to an environment ripe for compromise. Below, we dive into the contextual elements of these campaigns, and how they relate to a weakened security posture.

Contextual elements of ransomware campaigns

To successfully execute a ransomware campaign, criminals must gain access to the victim's system or device. In some.variants of these criminal schemes, access is actually purchased from other bad actors.



#379512 - NO REFUND FOR FRESH RDP!

$10
United States

Windows Server 2008 R2 Standard
Intel(R) Xeon(R) CPU E5-2407 0 @ 2.20GHz
Memory (RAM): -- | Cores: 4

Dwn. Speed: 6.52 Mbit/s | Upl. Speed: 4.57 Mbit/s

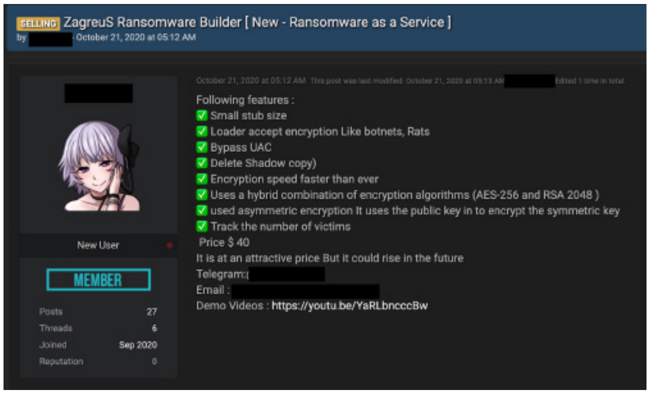
Admin Rights: ✓
Direct IP: ✗
Antivirus: Unknown Blacklist: Check
proxyScore: Check

Domain: *.
ISP: City

Browsers: Ie, Chrome
Payment Systems: Not found
Online Shops: Not found
Poker Rooms: Not found
Dating: Not found
Other Sites: Not found

Source: HelpnetSecurity

This means anyone can broker a campaign, regardless of their technical know-how. All they need to do is buy ransomware payloads from crimeware developers. The following screenshot goes to show the extent of the current ransomware market within the criminal underworld.



SELLING ZagreuS Ransomware Builder [New - Ransomware as a Service]
by [redacted] · October 21, 2020 at 05:12 AM

[redacted]

New User

MEMBER

Posts	27
Threads	6
Joined	Sep 2020
Reputation	0

October 21, 2020 at 05:12 AM · This post was last modified: October 21, 2020 at 05:13 AM [redacted] Edited 1 time in total.

Following features :
✓ Small stub size
✓ Loader accept encryption Like botnets, Rats
✓ Bypass UAC
✓ Delete Shadow copy)
✓ Encryption speed faster than ever
✓ Uses a hybrid combination of encryption algorithms (AES-256 and RSA 2048)
✓ used asymmetric encryption It uses the public key in to encrypt the symmetric key
✓ Track the number of victims
Price $ 40
It is at an attractive price But it could rise in the future
Telegram:[redacted]
Email : [redacted]
Demo Videos : https://youtu.be/YaRLbncccBw

Source: Recorded Future

During our research, we found several common elements that are present during ransomware campaigns and key to their success.

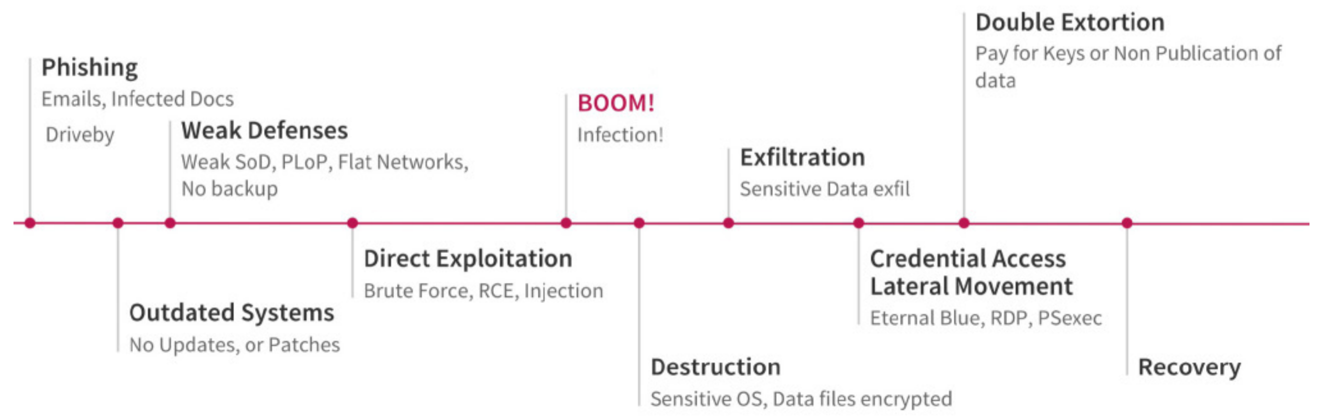
Initial access usually comes from delivering payloads associated with crimeware carriers like Trickbot. These carriers will include exploit code — a type of code that zeros in on security flaws and vulnerabilities — that are small in size, multi-staged and designed to bypass defenses. Once installed, more payloads will deploy, including additional exploits targeting other hosts. This allows the operator to move laterally across the system, exfiltrate data and install ransomware.

As mentioned earlier, ransomware can also be delivered via third-party vendors on various dark markets, brute-forcing internet servers with weak authentication mechanisms, and exploiting outdated, misconfigured or vulnerable operating systems and applications. Phishing attacks are another popular channel for ransomware, where bad actors will send emails (or another type of communication) to the victim, persuading or misleading them into opening the infected files. It's important to notice that sometimes the exploitation, exfiltration, lateral movement and infection may happen very close together once the malicious payload is executed.

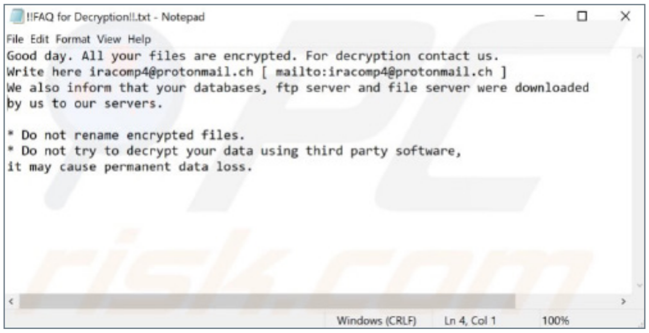
This is why it's so important for malicious actors to persuade victims to open malicious files and execute exploits. Recent reports indicate that malicious groups like FIN7 are also using physical deliveries accompanied by a letter (similar to the ones they send via email), a fake store card and USB a stick, as seen in the following picture.

Source: BankInfoSecurity

Once executed, these payloads will quickly proliferate across "flat" networks that have poor security and/or undiscriminating user privileges, where a host can gain access to any part of the organization's network, including administrative access to sensitive and critical files. If no data backups or recovery procedures exist, victims have no choice but to consider paying the ransom, as their business continuity has been compromised.



After BOOM

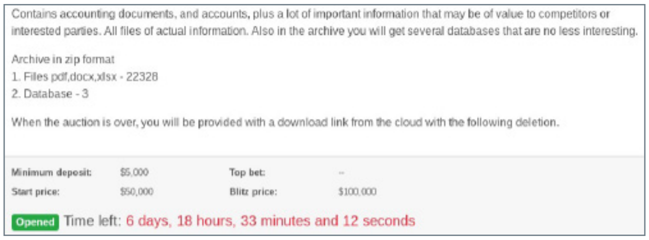

!!FAQ for Decryption!!.txt - Notepad
File Edit Format View Help
Windows (CRLF)
Ln 4, Col 1
100%

```
Good day. All your files are encrypted. For decryption contact us.
Write here iracomp4@protonmail.ch [ mailto:iracomp4@protonmail.ch ]
We also inform that your databases, ftp server and file server were downloaded
by us to our servers.

* Do not rename encrypted files.
* Do not try to decrypt your data using third party software,
it may cause permanent data loss.
```

Source: PCRisk

Once the infection has taken root, victims will receive a ransom note. This note will tell the victim to not decrypt the affected files, and will include a means of communicating with the perpetrators (usually an email address or site on the dark web). The ransomware operator's communications usually include a time by when the victim must pay the ransom, or the files will be published or destroyed.

Double extortion



Contains accounting documents, and accounts, plus a lot of important information that may be of value to competitors or interested parties. All files of actual information. Also in the archive you will get several databases that are no less interesting.

Archive in zip format
1. Files pdf,docx,xlsx - 22328
2. Database - 3

When the auction is over, you will be provided with a download link from the cloud with the following deletion.

Minimum deposit:	$5,000	Top bet:	–
Start price:	$50,000	Blitz price:	$100,000

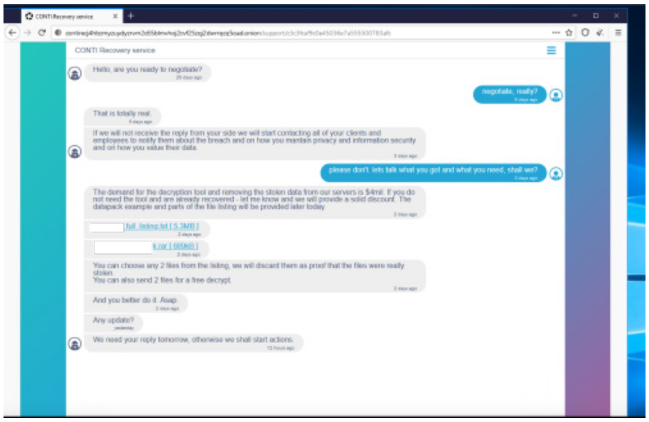
Opened Time left: 6 days, 18 hours, 33 minutes and 12 seconds

Source: Krebsonsecurity

As seen in the example above, this is a common element of malicious campaigns, where sensitive information is exfiltrated and placed for sale on the dark web or via data brokers on dark markets.

The exfiltration occurs some time after malicious actors have been able to exploit and execute code that will likely follow worm-like behavior when searching for additional hosts, testing permissions, accessing credentials, and attempting to use said credentials in every other system it can reach (via RDP, SMB or PSExec), executing additional exploits such as EternalBlue and finally applying ciphers to files, usually leaving affected systems barely functioning, with the ransom note on full display.

To pay or not to pay?



Hello, are you ready to negotiate?
28 days ago

negotiate, really?
6 days ago

That is totally real.
6 days ago

If we will not receive the reply from your side we will start contacting all of your clients and employees to notify them about the breach and on how you mantain privacy and information security and on how you value their data.
3 days ago

please don't. lets talk what you got and what you need, shall we?
2 days ago

The demand for the decryption tool and removing the stolen data from our servers is $4mil. If you do not need the tool and are already recovered - let me know and we will provide a solid discount. The datapack example and parts of the file listing will be provided later today
2 days ago

full_listing.txt [5.3MB]
2 days ago

k.rar [689kB]
2 days ago

You can choose any 2 files from the listing, we will discard them as proof that the files were really stolen.
You can also send 2 files for a free decrypt.
2 days ago

And you better do it. Asap.
2 days ago

Any update?
yesterday

We need your reply tomorrow, otherwise we shall start actions.
12 hours ago

This question presents an illusion of choice. If a company was compromised and all its systems were ciphered (in some cases, this can even extend to their backup servers), then the target has no choice but to pay the ransom. Especially when interruptions are a matter of life or death.

Unfortunately, the rate of recovery is unlikely to be 100 percent. It also takes considerable time to decrypt data, verify its integrity and restore the infrastructure and business operations to what they were.

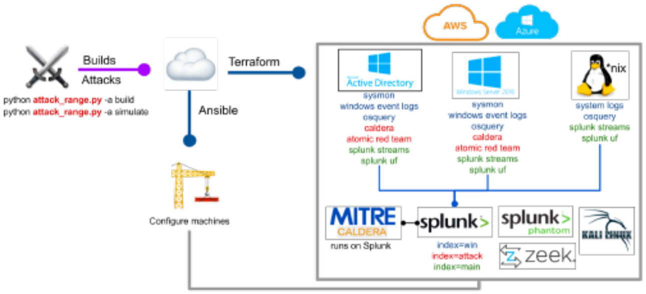
Methodology

Throughout our research, we used several tools — namely the Splunk Attack Range — to collect data from malicious payloads. Samples of Darkside, Clop, Ryuk, Conti and REvil were obtained from a Splunk partner, Reversing Labs. These variants were chosen based on ongoing campaign reports.

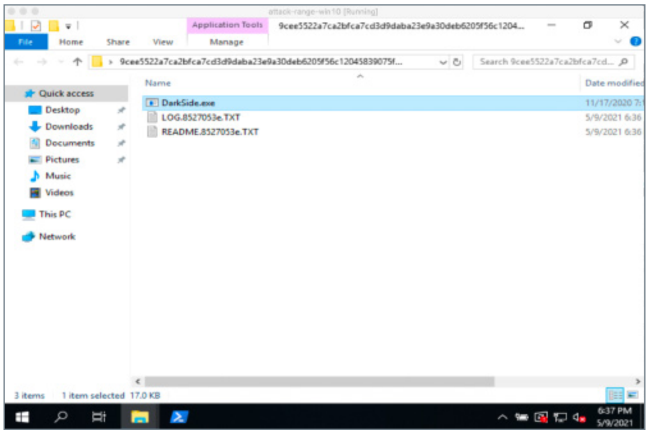
These samples were executed individually in Attack Range ephemeral environments. From there, we obtained data of execution via Sysmon data. We crafted streamlined SPL searches for all indicators of compromise (IOCs) or industry-defined techniques, tactics and procedures (i.e., the MITRE ATT&CK framework) observed from these deployments.

We then created analytic stories for each sample. An analytic story consists of several searches that work as individual indicators, and confirm the presence of threats when occurring in concert and within a proximate timing.

Below is an example of this methodology. First, we created a simulation by using Splunk Attack Range. In this environment, we can measure execution data from these payloads. The following diagram outlines the components of these environments created during our research of ransomware payloads. In the case of the aforementioned payloads, we used windows clients and servers to trigger execution and measure data from these attacks.

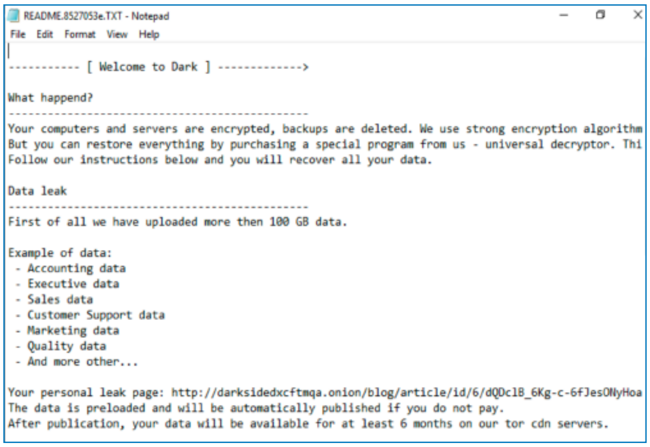


In the following screenshot sequence, we show how we replicated Darkside ransomware, which was the crimeware used against the colonial pipeline. After creating the environment, we proceeded to transfer samples to the targeted Windows 10 client. Then we proceeded to execute the sample. DarkSide ransomware first creates a log file followed by a victim ID and text extension, and also creates a readme text note with the ID.


attack-range-win10 [Running]
Application Tools
9cee5522a7ca2bfca7cd3d9daba23e9a30deb6205f56c1204...
File
Home
Share
View
Manage
9cee5522a7ca2bfca7cd3d9daba23e9a30deb6205f56c12045839075f...
Search 9cee5522a7ca2bfca7cd...
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
This PC
Network
3 items
1 item selected 17.0 KB
6:37 PM
5/9/2021

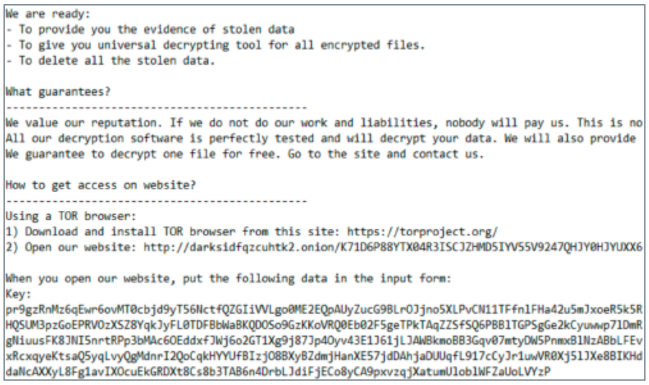
```
Name                        Date modified
DarkSide.exe                11/17/2020 7:
LOG.8527053e.TXT            5/9/2021 6:36
README.8527053e.TXT         5/9/2021 6:36
```

We then discovered the following in the readme. victimid.txt file.



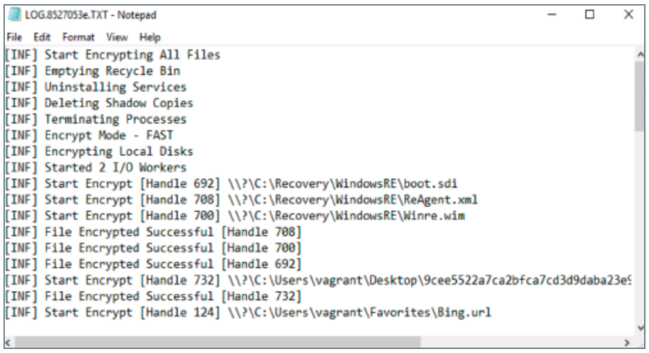
```
----------- [ Welcome to Dark ] ------------->

What happend?
----------------------------------------------
Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithm
But you can restore everything by purchasing a special program from us - universal decryptor. Thi
Follow our instructions below and you will recover all your data.

Data leak
----------------------------------------------
First of all we have uploaded more then 100 GB data.

Example of data:
 - Accounting data
 - Executive data
 - Sales data
 - Customer Support data
 - Marketing data
 - Quality data
 - And more other...

Your personal leak page: http://darksidedxcftmqa.onion/blog/article/id/6/dQDclB_6Kg-c-6fJesONyHoa
The data is preloaded and will be automatically published if you do not pay.
After publication, your data will be available for at least 6 months on our tor cdn servers.
```

As seen in the screenshot above, the attackers state that they have encrypted computers, servers and deleted any existing backup. Then, they claim that they have a significant amount of data from the customer, and provide an onion link leading to a page featuring samples of leaked data, along with a timeline for when they'll start releasing sensitive files. Finally, they provide instructions on how to pay the ransom, as seen below.



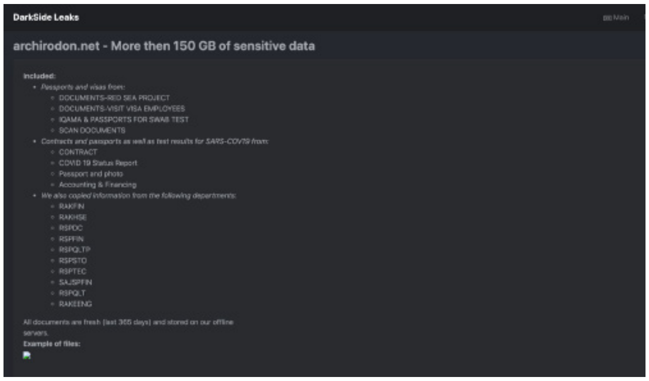
```
We are ready:
- To provide you the evidence of stolen data
- To give you universal decrypting tool for all encrypted files.
- To delete all the stolen data.

What guarantees?
----------------------------------------------
We value our reputation. If we do not do our work and liabilities, nobody will pay us. This is no
All our decryption software is perfectly tested and will decrypt your data. We will also provide
We guarantee to decrypt one file for free. Go to the site and contact us.

How to get access on website?
----------------------------------------------
Using a TOR browser:
1) Download and install TOR browser from this site: https://torproject.org/
2) Open our website: http://darksidfqzcuhtk2.onion/K71D6P88YTX04R3ISCJZHMD5IYV55V9247QHJY0HJYUXX6

When you open our website, put the following data in the input form:
Key:
pr9gzRnMz6qEwr6ovMT0cbjd9yT56NctfQZGIiVVLgo0ME2EQpAUyZucG9BLrOJjno5XLPvCN11TFfnlFHa42u5mJxoeR5k5R
HQSUM3pzGoEPRVOzXSZ8YqkJyFL0TDFBbWaBKQDOSo9GzKKoVRQ0Eb02F5geTPkTAqZZSfSQ6PBBlTGPSgGe2kCyuwwp71DmR
gNiuusFK8JNI5nrtRPp3bMAc6OEddxfJWj6o2GT1Xg9j87Jp4Oyv43E1J61jLJAWBkmoBB3Gqv07mtyDW5PnmxBlNzABbLFEv
xRcxqyeKtsaQ5yqLvyQgMdnrI2QoCqkHYYUfBIzjO8BXyBZdmjHanXE57jdDAhjaDUUqfL917cCyJr1uwVR0Xj51JXe8BIKHd
daNcAXXyL8Fg1avIXOcuEkGRDXt8Cs8b3TAB6n4DrbLJdiFjECo8yCA9pxvzqjXatumUloblWFZaUoLVYzP
```

The log.victim.txt also provides information about the files encrypted.



```
[INF] Start Encrypting All Files
[INF] Emptying Recycle Bin
[INF] Uninstalling Services
[INF] Deleting Shadow Copies
[INF] Terminating Processes
[INF] Encrypt Mode - FAST
[INF] Encrypting Local Disks
[INF] Started 2 I/O Workers
[INF] Start Encrypt [Handle 692] \\?\C:\Recovery\WindowsRE\boot.sdi
[INF] Start Encrypt [Handle 708] \\?\C:\Recovery\WindowsRE\ReAgent.xml
[INF] Start Encrypt [Handle 700] \\?\C:\Recovery\WindowsRE\Winre.wim
[INF] File Encrypted Successful [Handle 708]
[INF] File Encrypted Successful [Handle 700]
[INF] File Encrypted Successful [Handle 692]
[INF] Start Encrypt [Handle 732] \\?\C:\Users\vagrant\Desktop\9cee5522a7ca2bfca7cd3d9daba23e9
[INF] File Encrypted Successful [Handle 732]
[INF] Start Encrypt [Handle 124] \\?\C:\Users\vagrant\Favorites\Bing.url
```

After visiting a DarkSide group website, we found a pattern in identifying compromised companies and describing how much information they were able to obtain, including what they call "examples of files," which are displayed images of actual documents obtained from victims.



archirodon.net - More then 150 GB of sensitive data

Included:

- *Passports and visas from:*
  - DOCUMENTS-RED SEA PROJECT
  - DOCUMENTS-VISIT VISA EMPLOYEES
  - IQAMA & PASSPORTS FOR SWAB TEST
  - SCAN DOCUMENTS
- *Contracts and passports as well as test results for SARS-COVI9 from:*
  - CONTRACT
  - COVID 19 Status Report
  - Passport and photo
  - Accounting & Financing
- *We also copied information from the following departments:*
  - RAKFIN
  - RAKHSE
  - RSPDC
  - RSPFIN
  - RSPQLTP
  - RSPSTO
  - RSPTEC
  - SAJSPFIN
  - RSPQLT
  - RAKEENG

All documents are fresh (last 365 days) and stored on our offline servers.

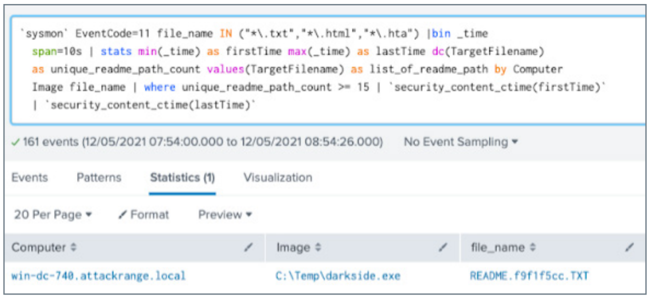
Example of files:

Once we ingested data from the payload execution in our Attack Range instance, we then crafted several searches that would be grouped into a single concept called an "Analytic Story." This helps us group together detections focusing on specific payloads – in this case, we created an Analytic Story focused on DarkSide ransomware.

The following screenshot is an example of one of these searches, along with the data obtained from executing the payload within our Attack Range environment. In the initial stages of execution, the payload creates readme files (i.e., the ransomware note) including the victim ID and text (.txt) file extension. One characteristic of this payload is the frequency at which these notes are created, and by using the Sysmon source type from our configured windows instance, we can craft a search around this feature.

```
`sysmon` EventCode=11 file_name IN ("*\.
txt","*\.html","*\.hta") |bin _time
  span=10s | stats min(_time) as firstTime
max(_time) as lastTime dc(TargetFilename)
  as unique_readme_path_count
values(TargetFilename) as list_of_readme_
path by Computer
  Image file_name | where unique_readme_
path_count >= 15 | `security_content_
ctime(firstTime)`
  | `security_content_ctime(lastTime)`
```

The next screenshot shows how it looks in Splunk.



```
`sysmon` EventCode=11 file_name IN ("*\.txt","*\.html","*\.hta") |bin _time
  span=10s | stats min(_time) as firstTime max(_time) as lastTime dc(TargetFilename)
  as unique_readme_path_count values(TargetFilename) as list_of_readme_path by Computer
  Image file_name | where unique_readme_path_count >= 15 | `security_content_ctime(firstTime)`
  | `security_content_ctime(lastTime)`
```

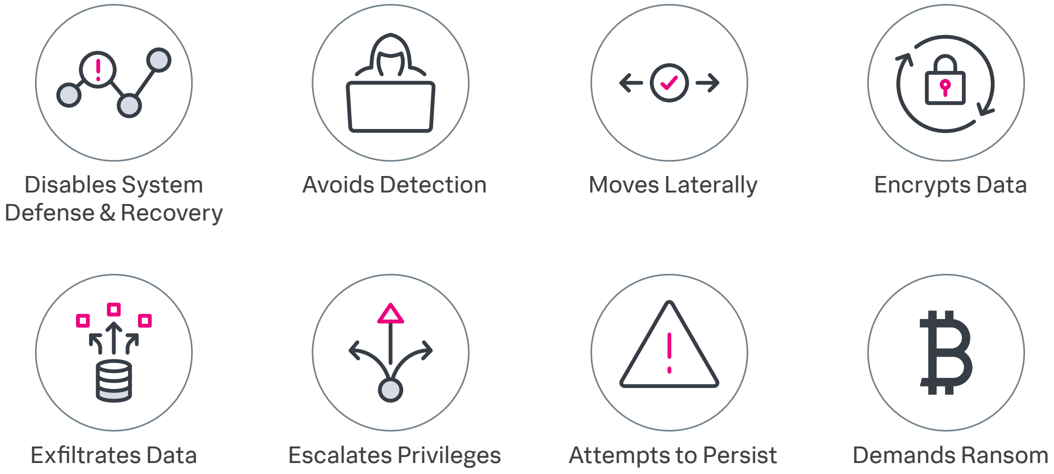
✓ 161 events (12/05/2021 07:54:00.000 to 12/05/2021 08:54:26.000)

Computer	Image	file_name
win-dc-740.attackrange.local	C:\Temp\darkside.exe	README.f9f1f5cc.TXT

There are dozens of searches included in this specific Analytic Story, which focus on DarkSide ransomware. This is just one example of how we conducted our research. The code for the above, as well as all the security content we produce, can be found on Splunk's security content GitHub or research microsite.

Commonalities

Based on our research from 2020-2021, we found several commonalities among the ransomware payloads observed. These commonalities are covered across eight categories, as seen in the following graphic.



To provide an understanding of these commonalities in industry terms, we've grouped them together using MITRE ATT&CK's nomenclature for reference and verification.

1. Encrypt data

Every single ransomware payload applies a cryptographic cipher to both user and system files, hindering or preventing host operations while disabling system defenses and recovery mechanisms (most operating systems have fail-safe mechanisms to recover from system file deletion). The following techniques can be found under the MITRE ATT&CK "impact" tactic.

T1485: Destroys data (via deletion or encryption)

Payloads encrypt user and system files preventing operation.

2. Disable system defenses and recovery

T1490: Inhibits system recovery for Windows OS. Payloads delete or disable shadow copy services to prevent the recovery of files.

3. Avoid detection

Payloads need to bypass security by circumventing monitoring and endpoint detection, as well as antivirus software, firewalls, process segmentation, and other operating system defenses (e.g., DEP, ASLR, SEHOP). These techniques can be found under the MITRE ATT&CK "defense evasion" tactic.

T1036.003: Renames binaries to avoid detection

T1070: Tampers with system files

T1070.001: Deletes logs

T1218.003: Abuses profile installers to execute code

T1562.001: Impairs defenses — disables or modifies tools

4. Move laterally

Another important feature of a successful ransomware campaign is the number of hosts and networks the infection can reach. One way to achieve this is by accessing credentials or exploiting vulnerable services, for example by extracting credentials from compromised hosts and then using them to access other hosts for example using Remote Desktop Access, or simply trying to access network shares to check for privileges and stored files. This category can be found under MITRE ATT&CK tactic "lateral movement."

T1021.002: Use of valid accounts in lateral movement

5. Exfiltration of data

Every successful ransomware campaign requires tracking the target in question; to do this, malicious actors have devised artifacts (i.e, the victim ID or underlying password hash) to track their victims, their data and — in many cases — the size of their ransom and payment management. These artifacts are either transmitted voluntarily when the victim enters the ID or hash.

As mentioned, some of these payloads are multistaged, and need some kind of telemetry to get to the next phase of the kill chain. This requires a connection via HTTP protocol — wrapped under an encryption layer like SSL or TLS — obfuscating operator actions and evading any proxy or deep packet inspection defense mechanisms.

Finally, to perform the double extortion scheme, the perpetrators obtain sensitive information regarding their target via command and control. Operators will transmit data from their victim's environments, methodologically searching for sensitive data. These actions can be found under the MITRE ATT&CK tactics "command and control," and "exfiltration."

T1071.001: Web traffic for execution, C2

T1048: Uses HTTPS for exfiltration

6. Escalate privileges

Achieving the highest privilege is necessary for many environments, especially corporate environments which have many layers of permissions and several network segments. This is why ransomware operators employ exploitation techniques — many of them taken from open source exploit sources — to escalate privileges when applicable.

There are many escalations of privilege techniques, but the ones present in all these payloads are the abuse of scheduled tasks and the creation of registry keys. These techniques can be found under the MITRE ATT&CK tactic "privilege escalation."

T1053: Use of Schedule tasks to escalate privileges

T1547.001: Use of boot/startup registry to escalate privileges

7. Attempts to persist

It's critical to remain on the host system in order to continue operations. In some cases, victims may even get lucky and delete ransomware binaries as they're executing, or execute antivirus or endpoint protection that may block or delete some of the payload's footprints. This is why persistence techniques are used to resist or bypass these defensive actions.

In this category, scheduled tasks check for the recurring execution of payloads. Many of these payloads have a footprint so extensive, that specific deletion techniques must be applied to clear the infection. These techniques can be found under the MITRE ATT&CK "persistence" tactic.

T1053: Use of Schedule tasks for code execution

T1547.001: Use of boot or log-on autostart execution — registry keys

8. Demand ransom

Ransom is usually required in the form of cryptocurrency — preferably in crypto coins such as Bitcoin, or any cryptocurrency that is harder to track than Zcash or Monero.

It is also important to note that besides the financial aspect in these campaigns, there have been other implicit factors inexorably tied to geopolitical variables, ultimately affecting the well-being of civilians (e.g., the shortage of fuel, disruptions in healthcare services, and other utilities).

According to the FBI, the definition of terrorism is "the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives" Ransomware is more than criminals asking for money — indeed, they use force against our property, our services and our livelihood. There are plenty of indicators pointing at historical and geopolitical factors driving these campaigns, however, these indicators are beyond the scope of this paper.

How can we better defend ourselves?

The Splunk Threat Research Team has developed extensive resources to detect and defend against ransomware. You can also find plenty of helpful information on the Cybersecurity and Infrastructure Security Agency (CISA) website. Finally, the following is some general guidance around preventing and defending against ransomware attacks:

- Ensure software is up-to-date, and prioritize patches to address known vulnerabilities.
- Splunk Enterprise Security Content Updates (ESCU) has extensive coverage of destructive software, including ransomware and crime carrier payloads. Download ESCU and perform preventative detection and monitoring of these threats.
- Test, verify and validate your perimeter defenses and remote access policies.
- Apply equivalent security policies from your organization's perimeter to your cloud resources.
- Confirm disaster recovery, business continuity and incident response resources on standby in case of intrusion or attack.
- Splunk SOAR has a playbook that focuses on detecting, containing and remediating ransomware.

Acknowledgments

This whitepaper could not have been accomplished without the help of the STRT team. I would like to thank the team for all their contributions.

- Teoderick Contreras
- Jose Hernandez
- Patrick Barreiss
- Lou Stella
- Mauricio Velazco
- Michael Haag
- Bhavin Patel
- Eric McGinnis

splunk>

Learn more: www.splunk.com/asksales

www.splunk.com