CybelAngel

itsa

Exposed Doors and Lost Keys

A new perspective on Proactive CyberSecurity

Thomas Garnier

Product Director at CybelAngel

Strategic Assets have become Digital

Web Apps

IoT

Code

Websites

Operational Technology

Personal Data

Risk have also become Digital

Web Apps

Fraud schemes

IoT

Phishing

Code

Economic Espionage

Websites

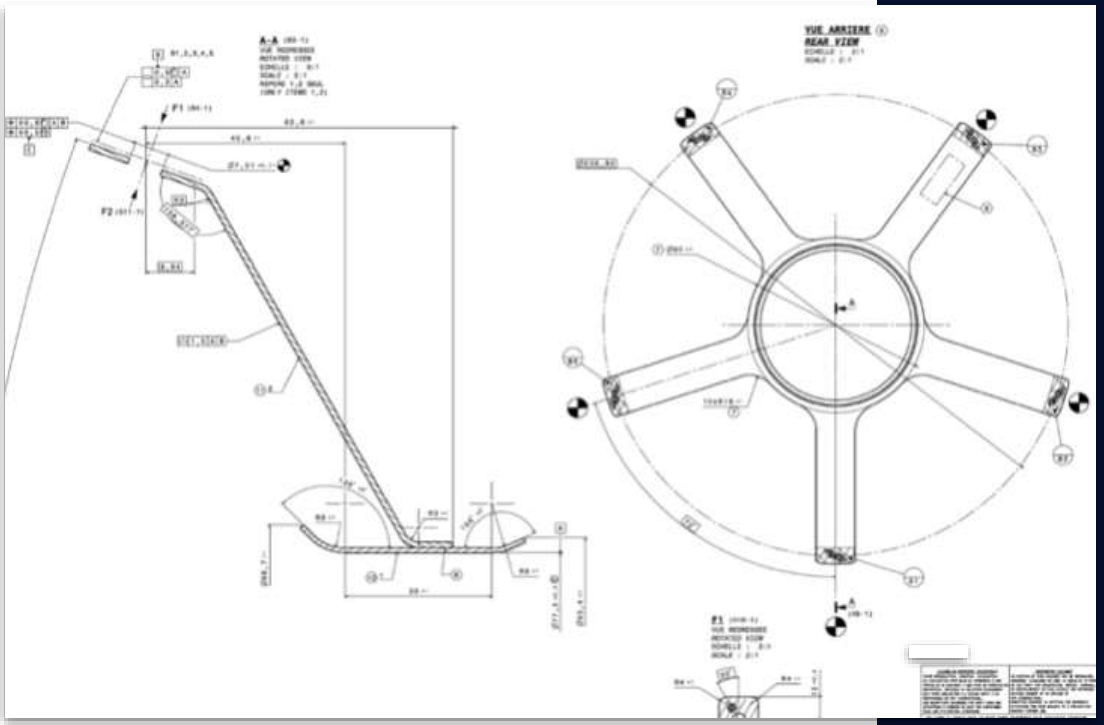
VIP Targeting

Operational Technology

Password Attack

Personal Data

Ransomware



Origin
Foreign Supplier — 3rd Party

Context
New, patented technology

Data types
Industrial drawings

Risks
Economic espionage, Ransomware

Assets are digital, Risk are digital.

Outside exposure keeps rising.

Developer outsourcing led to a **66% increase in source code leaks.**

Source: CybelAngel Industry Report 2021 / 2022

Outside exposure keeps rising.

GitHub

Developer outsourcing led to a **66% increase in source code leaks.**

Exposed credentials saw a 50% increase in "Major" incidents, i.e. those with a direct connection and an ability to damage a business.

Source: CybelAngel Industry Report 2021 / 2022

Outside exposure keeps rising.

GitHub

Developer outsourcing led to a **66% increase in source code leaks.**

Exposed credentials saw a 50% increase in "Major" incidents, i.e. those with a direct connection and an ability to damage a business.

Cloud storage leaks rose 150% due to remote work.

Source: CybelAngel Industry Report 2021 / 2022

Outside exposure keeps rising.

GitHub

Developer outsourcing led to a **66% increase in source code leaks.**

Exposed credentials saw a 50% increase in "Major" incidents, i.e. those with a direct connection and an ability to damage a business.

Cloud storage leaks rose 150% due to remote work.

40% growth in vulnerable shadow assets during H2 2021

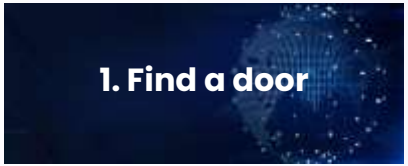
Source: CybelAngel Industry Report 2021 / 2022

What an attacker needs.

What an attacker needs.

Entry point

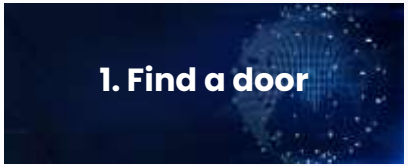
- a VPN
- an vulnerable RDP
- a misconfigured port
- an unsecured shadow asset
- a SaaS software
- a Cloud console

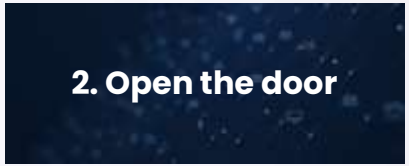


What an attacker needs.

Entry point
- a VPN
- an vulnerable RDP
- a misconfigured port
- an unsecured shadow asset
- a SaaS software
- a Cloud console

Access
- **A lost key**: credentials, cookies, etc.
- **A stolen key**: phishing campaign, etc.
- **A broken lock** : CVE



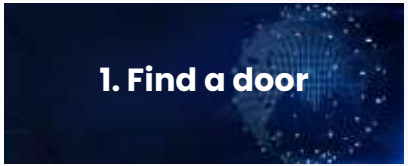


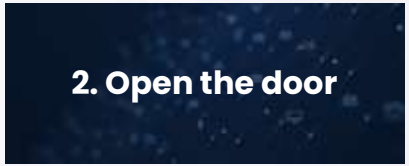
What an attacker needs.

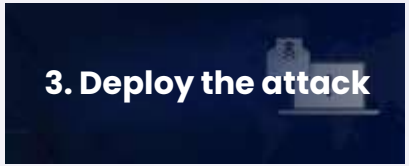
Entry point
- a VPN
- an vulnerable RDP
- a misconfigured port
- an unsecured shadow asset
- a SaaS software
- a Cloud console

Access
- **A lost key**: credentials, cookies, etc.
- **A stolen key**: phishing campaign, etc.
- **A broken lock** : CVE

- A **Malware**: Conti, Ragnar Locker, Alumni Locker, etc.
- The ability to **propagate** from one endpoint to the other







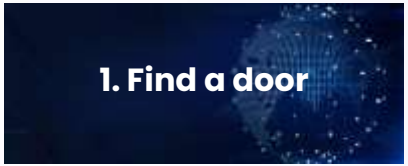
What an attacker needs.

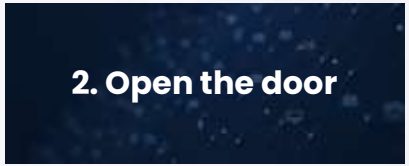
Entry point
- a VPN
- an vulnerable RDP
- a misconfigured port
- an unsecured shadow asset
- a SaaS software
- a Cloud console

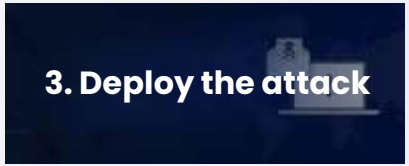
Access
- **A lost key**: credentials, cookies, etc.
- **A stolen key**: phishing campaign, etc.
- **A broken lock** : CVE

- A **Malware**: Conti, Ragnar Locker, Alumni Locker, etc.
- The ability to **propagate** from one endpoint to the other

- **Shutdown systems**
- **Encrypt** data
- **Sell** the data on the Dark Web







Zooming in on Preventive Strategies

Weak Entry Door

+

Break The Door

Ex: RDP/VPN exposed to CVEs

Re-use Lost Keys

Ex: Unsecure database leaking creds

Buy a Key

Ex: Creds for sale on the Dark Web

Steal a Key

Ex: Phishing campaign

No Key Required

Ex: Unprotected FTP server

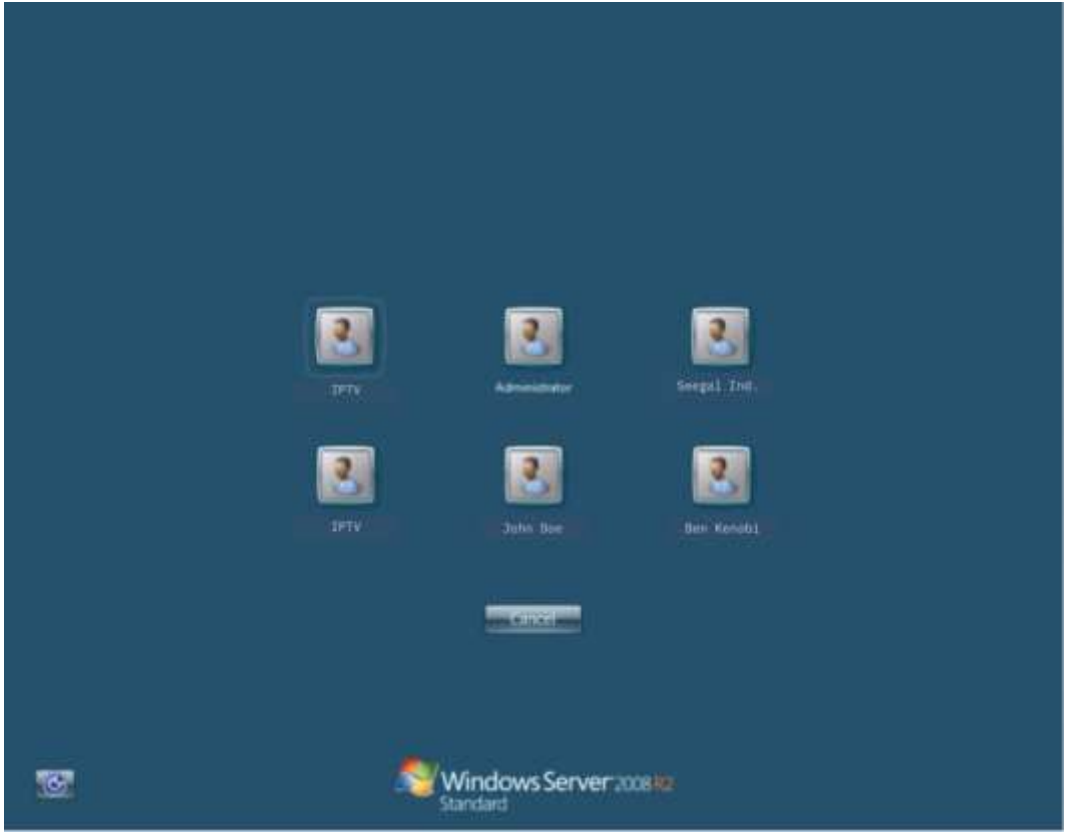
=

Business Damage


THE WALL STREET JOURNAL.

Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom

Example 0 — RDP server

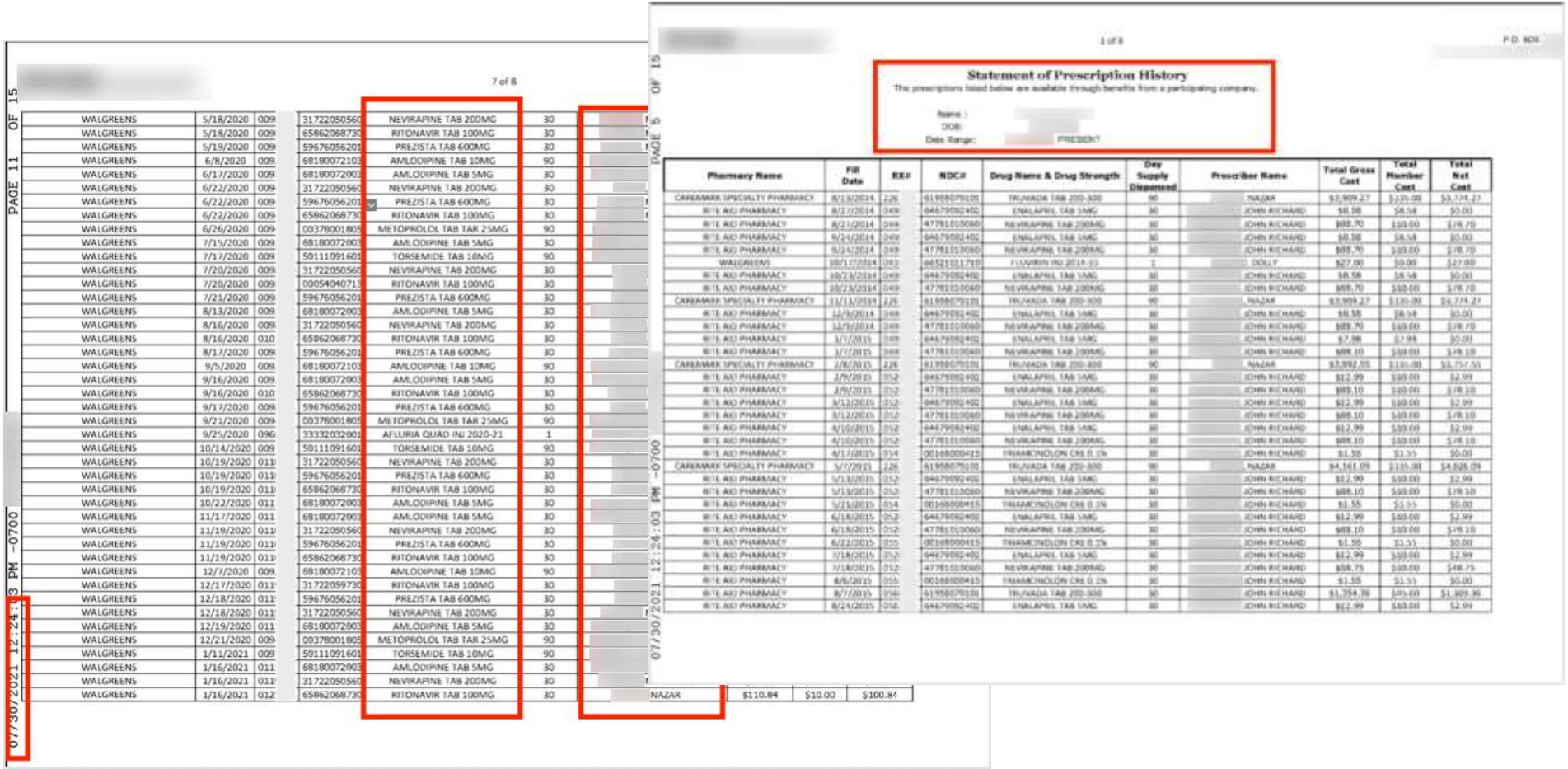


Example 1 — Login information

MySQL_29:01:2020_UserProfiles

```
1  abort-slave-event-count           0
2  allow-suspicious-udfs             FALSE
3  archive                           ON
4  auto-increment-increment          1
5  auto-increment-offset             1
6  autocommit                        TRUE
7  automatic-sp-privileges           TRUE
8  avoid-temporal-upgrade            FALSE
9  back-log                          80
10 basedir                           /home/jon/bin/mysql-5.7/
11
12
13 oliver.rivera@seegalindustries.com  passwordz
14 michael.hall@seegalindustries.com   password2
15 ben.campbell@seegalindustries.com   bestpassword
16 sophia.scott@seegalindustries.com   qwerty12345
17 abigail.ramirez@seegalindustries.com    azerty99
18 ben.hill@seegalindustries.com   17!lol22
19 abigail.campbell@seegalindustries.com   gamemars
20 isabella.perez@seegalindustries.com best?
21 sophia.young@seegalindustries.com   skatejohnwick
22 emma.hall@seegalindustries.com  13gates
23 oliver.allen@seegalindustries.com   07board
24 oliver.torres@seegalindustries.com  03cat
25 ethan.flores@seegalindustries.com   04fifa
26 sophia.robinson@seegalindustries.com    06boss
27 isabella.thompson@seegalindustries.com  02#zzzzz
28 mike.nelson@seegalindustries.com    17gates
29 ben.adams@seegalindustries.com  playermeta
```

Example 2 — Personal Health Information



7 of 8

WALGREENS	5/18/2020	009	31722050560	NEVIRAPINE TAB 200MG	30				
WALGREENS	5/18/2020	009	65862068730	RITONAVIR TAB 100MG	30				
WALGREENS	5/19/2020	009	59676056201	PREZISTA TAB 600MG	30				
WALGREENS	6/8/2020	009	68180072103	AMLODIPINE TAB 10MG	90				
WALGREENS	6/17/2020	009	68180072003	AMLODIPINE TAB 5MG	30				
WALGREENS	6/22/2020	009	31722050560	NEVIRAPINE TAB 200MG	30				
WALGREENS	6/22/2020	009	59676056201	PREZISTA TAB 600MG	30				
WALGREENS	6/22/2020	009	65862068730	RITONAVIR TAB 100MG	30				
WALGREENS	6/26/2020	009	00378001805	METOPROLOL TAB TAR 25MG	90				
WALGREENS	7/15/2020	009	68180072003	AMLODIPINE TAB 5MG	30				
WALGREENS	7/17/2020	009	50111091601	TORSEMIDE TAB 10MG	90				
WALGREENS	7/20/2020	009	31722050560	NEVIRAPINE TAB 200MG	30				
WALGREENS	7/20/2020	009	00054040713	RITONAVIR TAB 100MG	30				
WALGREENS	7/21/2020	009	59676056201	PREZISTA TAB 600MG	30				
WALGREENS	8/13/2020	009	68180072003	AMLODIPINE TAB 5MG	30				
WALGREENS	8/16/2020	009	31722050560	NEVIRAPINE TAB 200MG	30				
WALGREENS	8/16/2020	010	65862068730	RITONAVIR TAB 100MG	30				
WALGREENS	8/17/2020	009	59676056201	PREZISTA TAB 600MG	30				
WALGREENS	9/5/2020	009	68180072103	AMLODIPINE TAB 10MG	90				
WALGREENS	9/16/2020	009	68180072003	AMLODIPINE TAB 5MG	30				
WALGREENS	9/16/2020	010	65862068730	RITONAVIR TAB 100MG	30				
WALGREENS	9/17/2020	009	59676056201	PREZISTA TAB 600MG	30				
WALGREENS	9/21/2020	009	00378001805	METOPROLOL TAB TAR 25MG	90				
WALGREENS	9/25/2020	096	33332032001	AFLURIA QUAD INJ 2020-21	1				
WALGREENS	10/14/2020	009	50111091601	TORSEMIDE TAB 10MG	90				
WALGREENS	10/19/2020	011	31722050560	NEVIRAPINE TAB 200MG	30				
WALGREENS	10/19/2020	011	59676056201	PREZISTA TAB 600MG	30				
WALGREENS	10/19/2020	011	65862068730	RITONAVIR TAB 100MG	30				
WALGREENS	10/22/2020	011	68180072003	AMLODIPINE TAB 5MG	30				
WALGREENS	11/17/2020	011	68180072003	AMLODIPINE TAB 5MG	30				
WALGREENS	11/19/2020	011	31722050560	NEVIRAPINE TAB 200MG	30				
WALGREENS	11/19/2020	011	59676056201	PREZISTA TAB 600MG	30				
WALGREENS	11/19/2020	011	65862068730	RITONAVIR TAB 100MG	30				
WALGREENS	12/7/2020	009	68180072103	AMLODIPINE TAB 10MG	90				
WALGREENS	12/17/2020	011	31722059730	RITONAVIR TAB 100MG	30				
WALGREENS	12/18/2020	011	59676056201	PREZISTA TAB 600MG	30				
WALGREENS	12/18/2020	011	31722050560	NEVIRAPINE TAB 200MG	30				
WALGREENS	12/19/2020	011	68180072003	AMLODIPINE TAB 5MG	30				
WALGREENS	12/21/2020	009	00378001805	METOPROLOL TAB TAR 25MG	90				
WALGREENS	1/11/2021	009	50111091601	TORSEMIDE TAB 10MG	90				
WALGREENS	1/16/2021	011	68180072003	AMLODIPINE TAB 5MG	30				
WALGREENS	1/16/2021	011	31722050560	NEVIRAPINE TAB 200MG	30				
WALGREENS	1/16/2021	012	65862068730	RITONAVIR TAB 100MG	30		NAZAR	$110.84	$10.00	$100.84

1 of 8

Statement of Prescription History

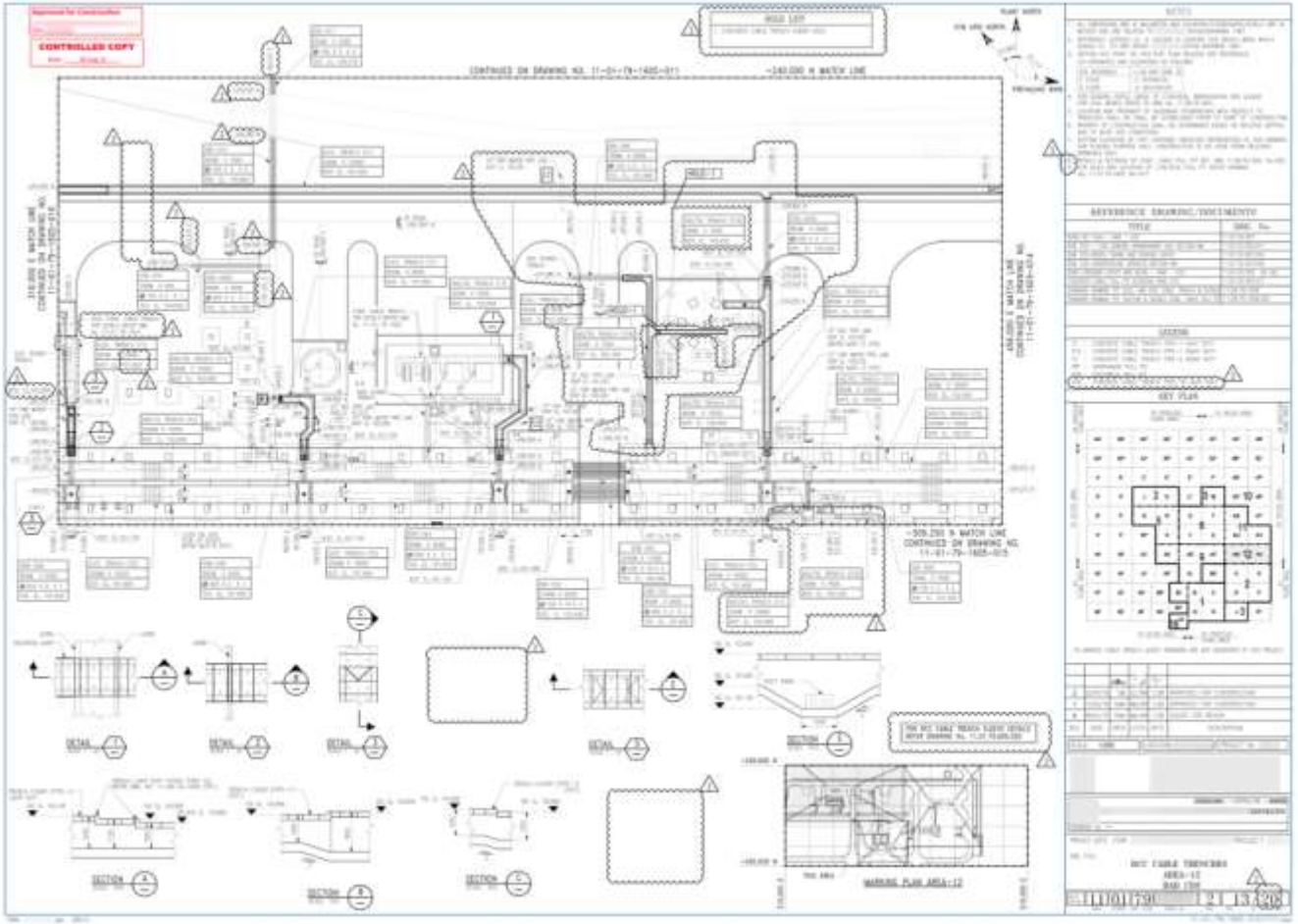
The prescriptions listed below are available through benefits from a participating company.

Name :
DOB:
Date Range: PRESENT

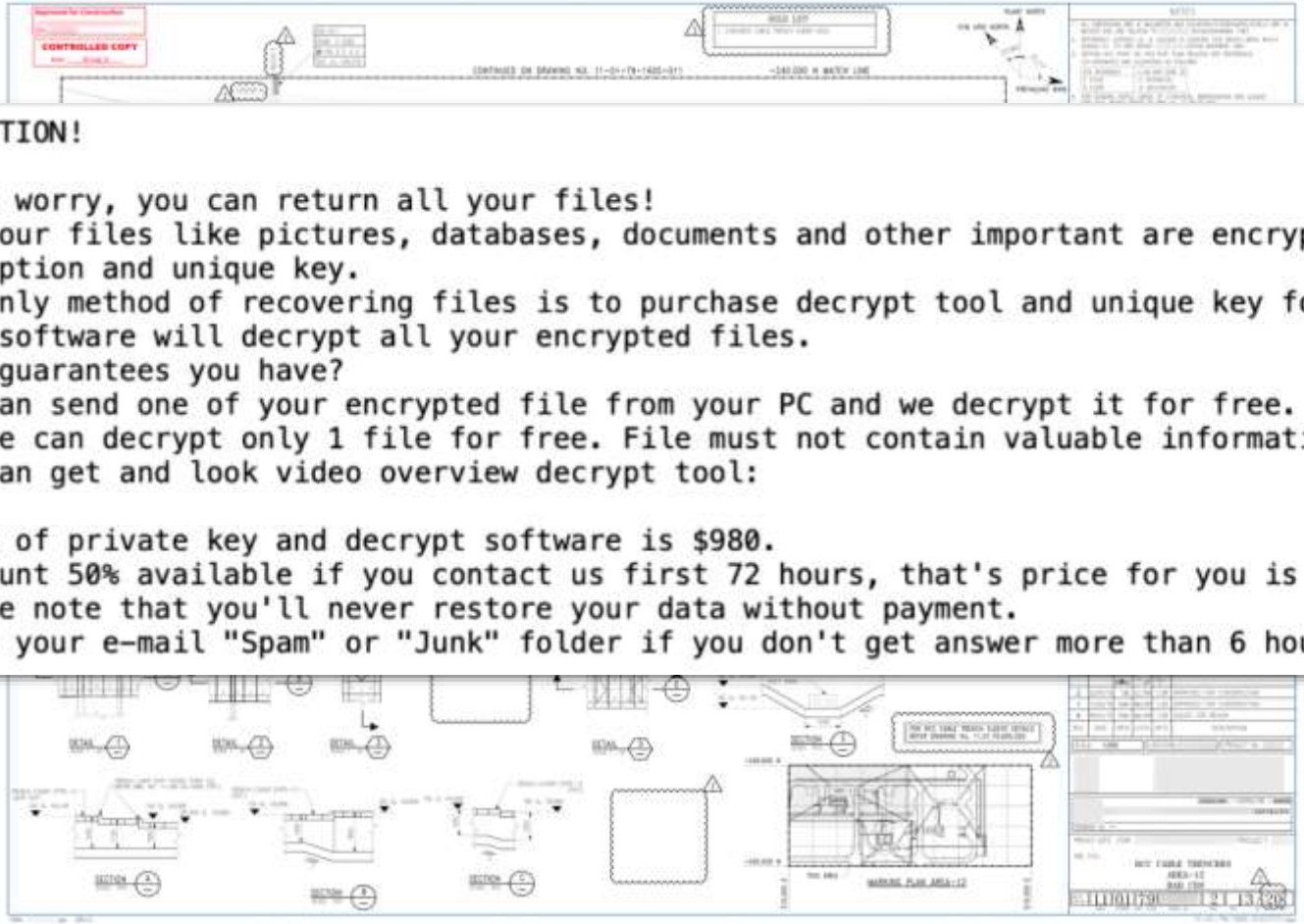
Pharmacy Name	Fill Date	RX#	NDC#	Drug Name & Drug Strength	Day Supply Dispensed	Prescriber Name	Total Gross Cost	Total Member Cost	Total Net Cost
CAREMARK SPECIALTY PHARMACY	8/13/2014	226	61958070101	TRIVADA TAB 200-300	90	NAZAR	$3,909.27	$135.00	$3,774.27
RITE AID PHARMACY	8/13/2014	349	67479082402	ENALAPRIL TAB 5MG	30	JOHN RICHARD	$8.58	$8.58	$0.00
RITE AID PHARMACY	8/23/2014	349	47781010060	NEVIRAPINE TAB 200MG	30	JOHN RICHARD	$88.70	$10.00	$78.70
RITE AID PHARMACY	9/24/2014	349	67479082402	ENALAPRIL TAB 5MG	30	JOHN RICHARD	$8.58	$8.58	$0.00
RITE AID PHARMACY	9/24/2014	349	47781010060	NEVIRAPINE TAB 200MG	30	JOHN RICHARD	$88.70	$10.00	$78.70
WALGREENS	10/17/2014	042	66521013710	FLUVIRIN INJ 2014-15	1	DOLLY	$27.00	$0.00	$27.00
RITE AID PHARMACY	10/23/2014	349	67479082402	ENALAPRIL TAB 5MG	30	JOHN RICHARD	$8.58	$8.58	$0.00
RITE AID PHARMACY	10/23/2014	349	47781010060	NEVIRAPINE TAB 200MG	30	JOHN RICHARD	$88.70	$10.00	$78.70
CAREMARK SPECIALTY PHARMACY	11/11/2014	226	61958070101	TRIVADA TAB 200-300	90	NAZAR	$3,909.27	$135.00	$3,774.27
RITE AID PHARMACY	12/9/2014	349	67479082402	ENALAPRIL TAB 5MG	30	JOHN RICHARD	$8.58	$8.58	$0.00
RITE AID PHARMACY	12/9/2014	349	47781010060	NEVIRAPINE TAB 200MG	30	JOHN RICHARD	$88.70	$10.00	$78.70
RITE AID PHARMACY	1/1/2015	349	67479082402	ENALAPRIL TAB 5MG	30	JOHN RICHARD	$7.98	$7.98	$0.00
RITE AID PHARMACY	1/1/2015	349	47781010060	NEVIRAPINE TAB 200MG	30	JOHN RICHARD	$88.10	$10.00	$78.10
CAREMARK SPECIALTY PHARMACY	2/6/2015	226	61958070101	TRIVADA TAB 200-300	90	NAZAR	$3,982.55	$135.00	$3,757.55
RITE AID PHARMACY	2/9/2015	352	67479082402	ENALAPRIL TAB 5MG	30	JOHN RICHARD	$12.99	$10.00	$2.99
RITE AID PHARMACY	2/9/2015	352	47781010060	NEVIRAPINE TAB 200MG	30	JOHN RICHARD	$88.10	$10.00	$78.10
RITE AID PHARMACY	3/12/2015	352	67479082402	ENALAPRIL TAB 5MG	30	JOHN RICHARD	$12.99	$10.00	$2.99
RITE AID PHARMACY	3/12/2015	352	47781010060	NEVIRAPINE TAB 200MG	30	JOHN RICHARD	$88.10	$10.00	$78.10
RITE AID PHARMACY	4/10/2015	352	67479082402	ENALAPRIL TAB 5MG	30	JOHN RICHARD	$12.99	$10.00	$2.99
RITE AID PHARMACY	4/10/2015	352	47781010060	NEVIRAPINE TAB 200MG	30	JOHN RICHARD	$88.10	$10.00	$78.10
RITE AID PHARMACY	4/11/2015	354	00168000415	FRAMECINOLON CRE 0.1%	30	JOHN RICHARD	$1.55	$1.55	$0.00
CAREMARK SPECIALTY PHARMACY	5/7/2015	226	61958070101	TRIVADA TAB 200-300	90	NAZAR	$4,161.09	$135.00	$4,026.09
RITE AID PHARMACY	5/13/2015	352	67479082402	ENALAPRIL TAB 5MG	30	JOHN RICHARD	$12.99	$10.00	$2.99
RITE AID PHARMACY	5/13/2015	352	47781010060	NEVIRAPINE TAB 200MG	30	JOHN RICHARD	$88.10	$10.00	$78.10
RITE AID PHARMACY	5/21/2015	354	00168000415	FRAMECINOLON CRE 0.1%	30	JOHN RICHARD	$1.55	$1.55	$0.00
RITE AID PHARMACY	6/18/2015	352	67479082402	ENALAPRIL TAB 5MG	30	JOHN RICHARD	$12.99	$10.00	$2.99
RITE AID PHARMACY	6/18/2015	352	47781010060	NEVIRAPINE TAB 200MG	30	JOHN RICHARD	$88.10	$10.00	$78.10
RITE AID PHARMACY	6/22/2015	355	00168000415	FRAMECINOLON CRE 0.1%	30	JOHN RICHARD	$1.55	$1.55	$0.00
RITE AID PHARMACY	7/18/2015	352	67479082402	ENALAPRIL TAB 5MG	30	JOHN RICHARD	$12.99	$10.00	$2.99
RITE AID PHARMACY	7/18/2015	352	47781010060	NEVIRAPINE TAB 200MG	30	JOHN RICHARD	$98.75	$10.00	$88.75
RITE AID PHARMACY	8/6/2015	355	00168000415	FRAMECINOLON CRE 0.1%	30	JOHN RICHARD	$1.55	$1.55	$0.00
RITE AID PHARMACY	8/7/2015	356	61958070101	TRIVADA TAB 200-300	90	JOHN RICHARD	$1,394.36	$35.00	$1,359.36
RITE AID PHARMACY	8/24/2015	356	67479082402	ENALAPRIL TAB 5MG	30	JOHN RICHARD	$12.99	$10.00	$2.99

PAGE 11 OF 15
07/30/2021 12:24:13 PM -0700
PAGE 5 OF 15
07/30/2021 12:24:13 PM -0700

Example 3 — Physical Security



Example 3 — Physical Security



```
ATTENTION!

Don't worry, you can return all your files!
All your files like pictures, databases, documents and other important are encrypted with strongest
encryption and unique key.
The only method of recovering files is to purchase decrypt tool and unique key for you.
This software will decrypt all your encrypted files.
What guarantees you have?
You can send one of your encrypted file from your PC and we decrypt it for free.
But we can decrypt only 1 file for free. File must not contain valuable information.
You can get and look video overview decrypt tool:

Price of private key and decrypt software is $980.
Discount 50% available if you contact us first 72 hours, that's price for you is $490.
Please note that you'll never restore your data without payment.
Check your e-mail "Spam" or "Junk" folder if you don't get answer more than 6 hours.
```

CybelAngel EASM[X]

Because you can't protect what you can't see.

Asset Discovery & Monitoring

Detect and secure **vulnerable shadow services** before they are hacked.

Sources include:

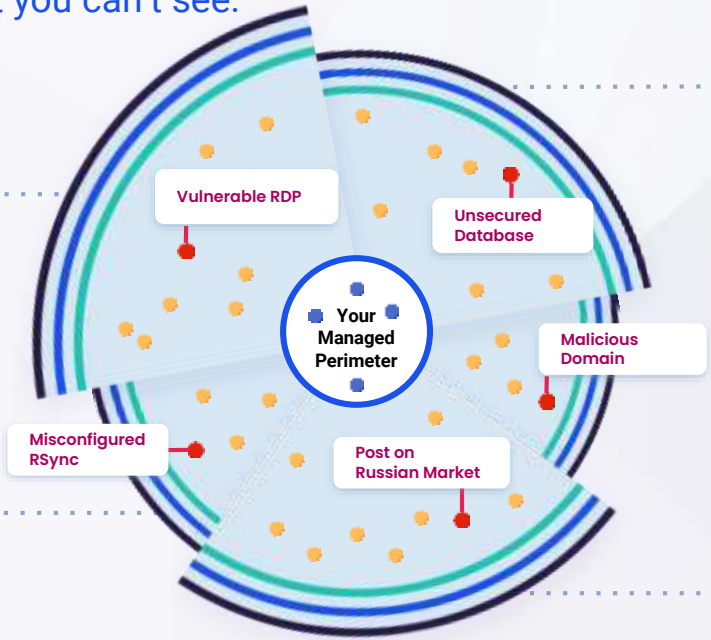
RDP TeamViewer Modbus Fox
Bacnet Dicom Telnet Docker

Data Breach Prevention

Monitor, detect, and secure publicly-accessible sensitive data before they are breached.

Sources include:

SMB FTP(S) GCS AWS S3 MySQL
Azure Storage ElasticSearch MongoDB



Account Takeover Prevention

Monitor and detect critical **credentials leaks** before they are compromised.

Sources include:

Open databases Public leaks Paste sites
Ransomware gangs Criminal marketplaces

Domain Protection

Monitor, detect, and take down **malicious domains** to keep your brand secure.

Sources include:

Zone files Passive DNS feeds
Certificate transparency logs

Dark Web Monitoring

Detect and mitigate targeted attacks planned on Dark Web forums, messaging apps, etc.

Sources include:

Tor forums Boards IRC
Telegram Discord

In-depth IPV4 & virtual host scanning

ML-powered filtering

Investigation & contextualization

Early Detection

Visualize all of External Attack Surface

Scan, Filter, Investigate findings

Remediation

Always think end-to-end protection

Integrate with your incident response processes.

Prioritization

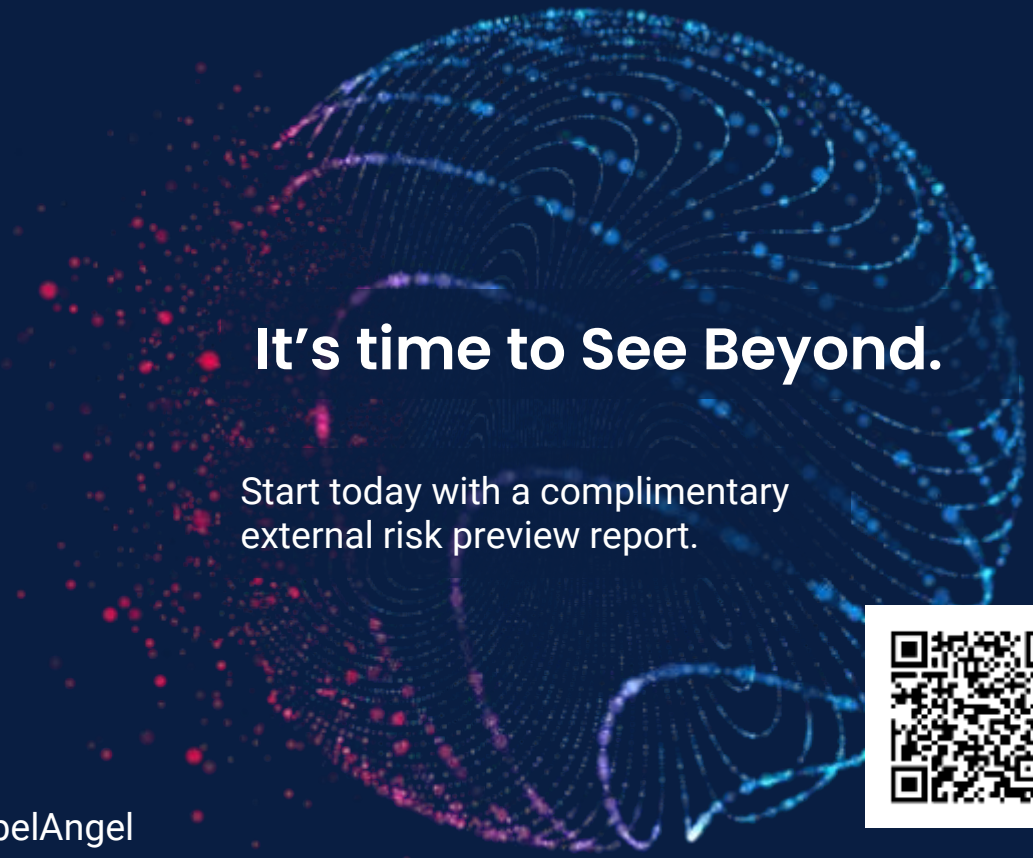
Assess Breach Likelihood and Business Impact with dedicated Analyst

Solving External Risks through Proactive Security

CybelAngel

Thank you!

Visit us at 7A-214.



Thomas Garnier, Product Director at CybelAngel

discover.cybelangel.com/external-risk-preview-report