Acronis Cyber Protect

AI-Powered Integration of Data Protection with Cybersecurity

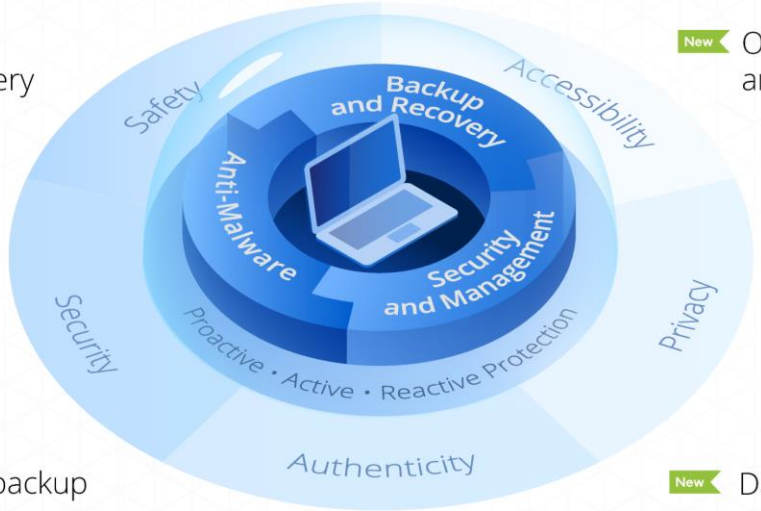
Integrated: ✓Licensing, ✓UI, ✓Management, ✓Agents & Backends, ✓Technology

New Anti-malware updates and patching during recovery

New Auto-adjust patching, scanning and backup to security alarms

New Automatically backup endpoints before installing any patches

New Forensic backup



New Offload and enable more aggressive scans and vulnerability assessments in backups

New Next-gen Continuous Data Protection

New Automated app whitelisting from backups

New Data protection map

Acronis Cyber Protect Cloud certified in VB100 tests by getting a 100% detection rate with zero false alarms

Acronis Cyber Protect

Windows 7 version	12.5.22410
Windows 10 version	12.5.22410
WildList detection	100.0%
False positive rate	0.000%
Diversity Test rate	98.35%

vb 100 June 2020 VIRUS virusbtn.com

Acronis joined the yearly certification round of Virus Bulletin VB100 tests and got a 100% detection rate and zero false detections in the first round. The VB100 award given (if certification passed) is a basic standard required for a security product to be recognized as legitimate and properly functioning anti-malware solutions. British Virus Bulletin was launched almost two decades ago and is one of the world leaders in security software testing.

1,325 views | Jun 16, 2020, 10:24am EDT

AFC Ajax Selects Acronis Over McAfee, Symantec And Trend Micro For Cyber Security

Sooraj Shah Contributor

Enterprise & Cloud

Acronis Cyber Protect happy customers

Manchester City F.C.

English Premier League champion in 2018 and 2019; one of the most successful teams in England based on trophy count with twenty-six major domestic and European honours.

Cobweb Solutions Ltd

Europe's largest Hosted Exchange provider. The first provider to deliver a customer through the Microsoft Cloud Solution Provider program.

BioConnect

Developer of biometric software and hardware designed for identifying employees and accessing their time and attendance.

Dallas Stars

Professional ice hockey team based in Dallas. Stanley Cup winner in 1998, one of Top-8 teams in 2019 season

Advanced Data Systems Corporation

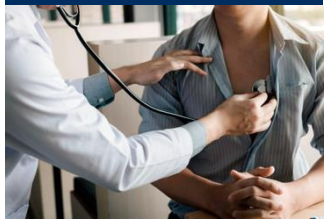
A leading provider of Electronic Health Records, Practice Management and Radiology Information Systems solutions, serving over 30,000 physicians and healthcare providers

Acronis Cyber Protection

All Acronis Products Combine AI-enhanced Data Protection and Security

Proactive Protection

Vulnerability assessment, patch and configuration management



Active Protection

Malware and in-memory defense, entropy analysis, self-protection

Reactive Protection

Fast automated backup, migration, disaster recovery and forensics

Cyber Notary

Digital identify for data powered by Blockchain

Cyber Privacy

Architecture designed for privacy and flexibility

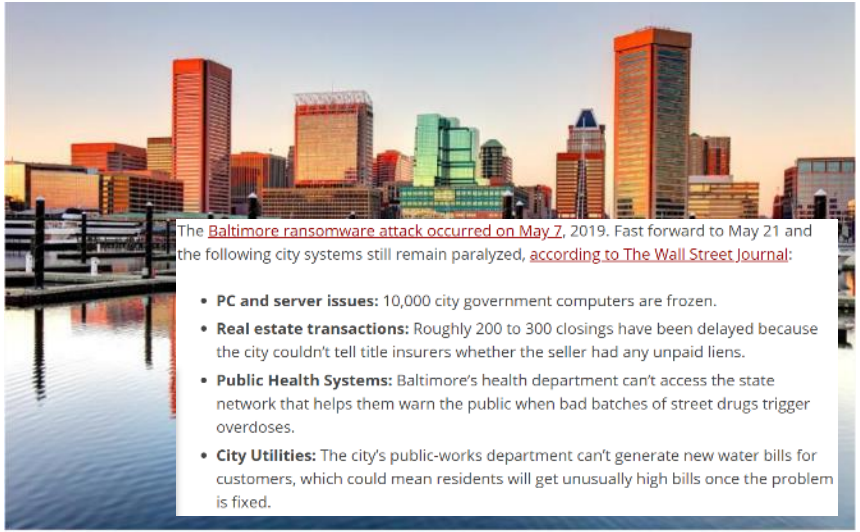
Sell Security? Move to Acronis Cyber Protect

Unique Capabilities: The most complete cyber protection for MSPs

Protection	Security	Performance
▪ Protection for collaboration applications – Zoom, WebEx, Microsoft teams ▪ AI-based hard-drive failure prediction ▪ Integrated protected file sync and share solution for collaboration	▪ AI-based injection detection ▪ Entropy analysis against advanced ransomware ▪ Rootkit detection by scanning cold backup data ▪ Aggressive heuristics enabled by whitelists created from backups	▪ Antivirus scans in backups, decreasing load on protected device ▪ Reduced downtime with fail-safe patch management ▪ Whitelisting applications by scanning backups

Productivity Benefits	
	▪ Quick assessment of a device protection status with built-in #CyberFit score ▪ Data protection map to discover and protect important data ▪ RDP connection to corporate networks for end customers

(2019): Recent attacks: Baltimore, Texas, Wisconsin



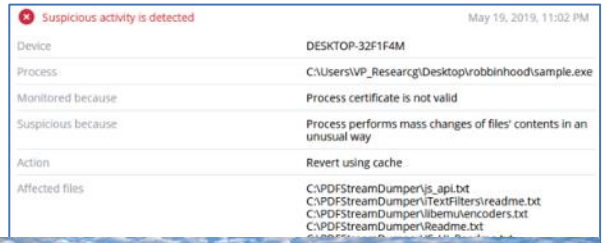
The Baltimore ransomware attack occurred on May 7, 2019. Fast forward to May 21 and the following city systems still remain paralyzed, according to The Wall Street Journal:

- **PC and server issues:** 10,000 city government computers are frozen.
- **Real estate transactions:** Roughly 200 to 300 closings have been delayed because the city couldn't tell title insurers whether the seller had any unpaid liens.
- **Public Health Systems:** Baltimore's health department can't access the state network that helps them warn the public when bad batches of street drugs trigger overdoses.
- **City Utilities:** The city's public-works department can't generate new water bills for customers, which could mean residents will get unusually high bills once the problem is fixed.

Baltimore is the latest U.S. city to fall prey to a virulent strain of ransomware attacks targeting the public sector. GETTY

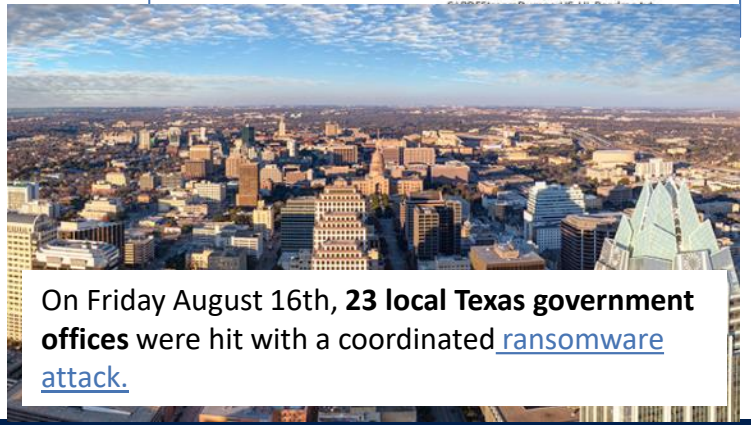
PerCSoft, a **Wisconsin-based** company that manages a remote data backup service relied upon by hundreds of dental offices across the country, is struggling to restore access to client systems after falling victim to a ransomware attack: the ransomware encrypted files for approximate **400 dental practices**

Acronis technologies deal with all 3 cases from day 0, providing full protection while the threat was not detected by a lot of antiviruses for a very long time!



Suspicious activity is detected — May 19, 2019, 11:02 PM

Device	DESKTOP-32F1F4M
Process	C:\Users\VP_Researcg\Desktop\robbinhood\sample.exe
Monitored because	Process certificate is not valid
Suspicious because	Process performs mass changes of files' contents in an unusual way
Action	Revert using cache
Affected files	C:\PDFStreamDumper\js_api.txt C:\PDFStreamDumper\iTextFilters\readme.txt C:\PDFStreamDumper\libemu\encoders.txt C:\PDFStreamDumper\Readme.txt

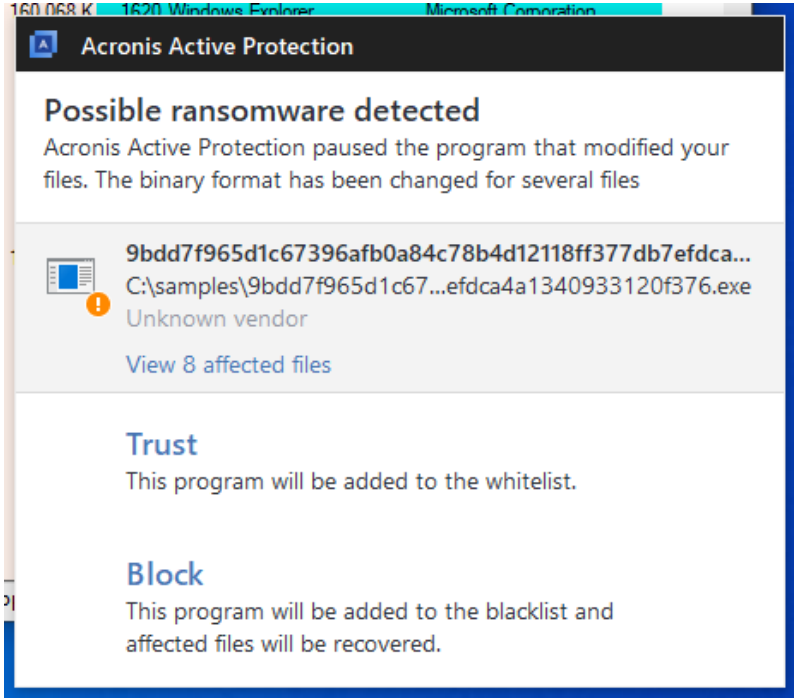


On Friday August 16th, **23 local Texas government offices** were hit with a coordinated ransomware attack.

April-May 2020: Key threats detection

April 2020: Energy Sector Giant Struck by $11M Ransomware Demand

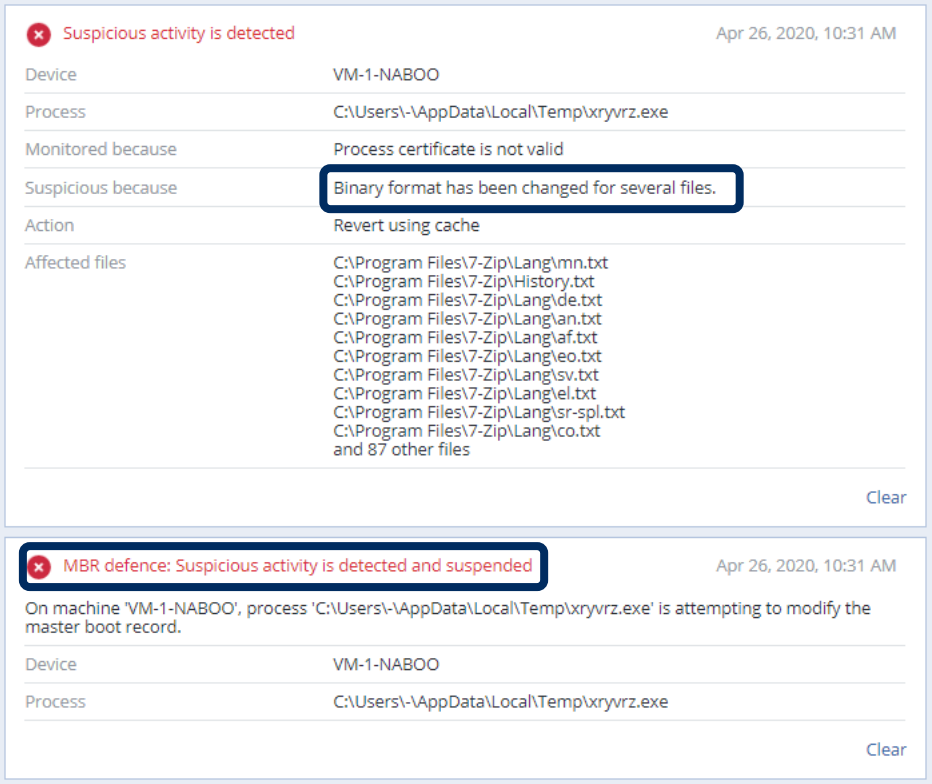
- Energias de Portugal (EDP) was attacked by cybercriminals using the recently unveiled ransomware strain Ragnar Locker. EDP is a multinational organization in the energy sector with a presence in 19 countries, a workforce of 11,500, and a customer base of more than 11 million depending on their energy production.



April-May 2020: Key threats detection

April 2020: Digital CoronaVirus: Yet Another Ransomware Combined with Infostealer

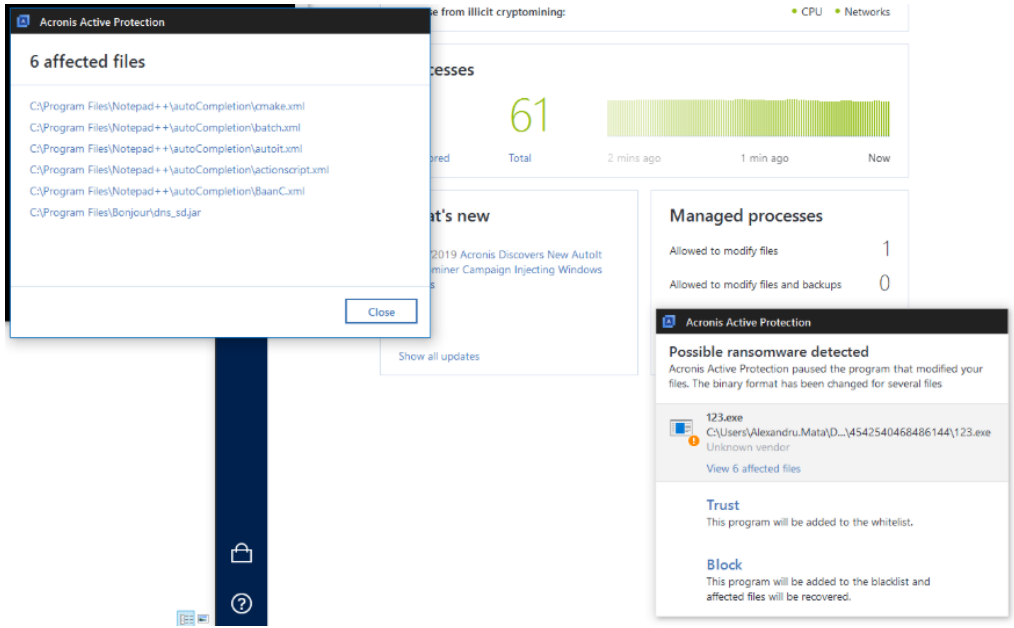
- This simple CoronaVirus example shows that cybercriminals other than those groups are trying to maximizing their profits as well. This is not a new strategy, a few years ago we saw ransomware attacks installing financial trojans and password stealers as well. The encryption attack could be a diversion, drawing attention away from the data leak, or it could be an attempt to increase the total profits.



April-May 2020: Key threats detection

May 2020: Snake ransomware leaks patient data from Fresenius Medical Care

- Fresenius is a large private hospital operator in Europe and its systems **were compromised as part of a** massive campaign from Snake ransomware that targeted organizations across all verticals.

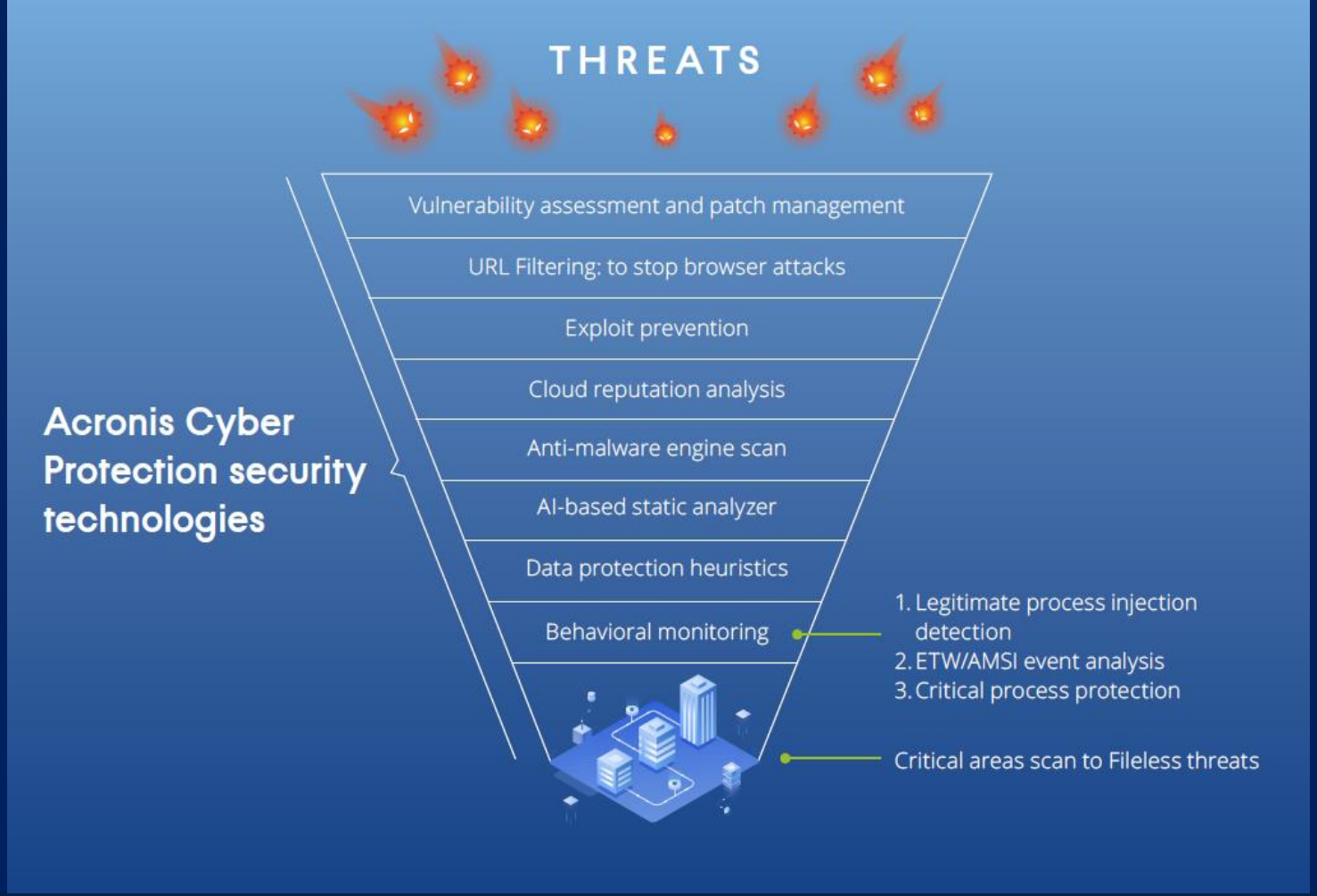


June: Knoxville is the 51st city to be hit in 2020

- **Knoxville Ransomware Attack Leads to IT Network Shutdown (Link)**The city of Knoxville Tennessee fell victim to a ransomware attack on June 12th which caused a large network outage including inhibiting law Enforcement to respond to non-life threatening incidents
- Initial investigations point to a spear phishing email attack that an official state employee had opened
- The city hired consultants estimate that the ransomware is most likely Maze, DoppelPaymer or NetWalker all of which, the ransomware protection in Acronis Cyber Protect can stop

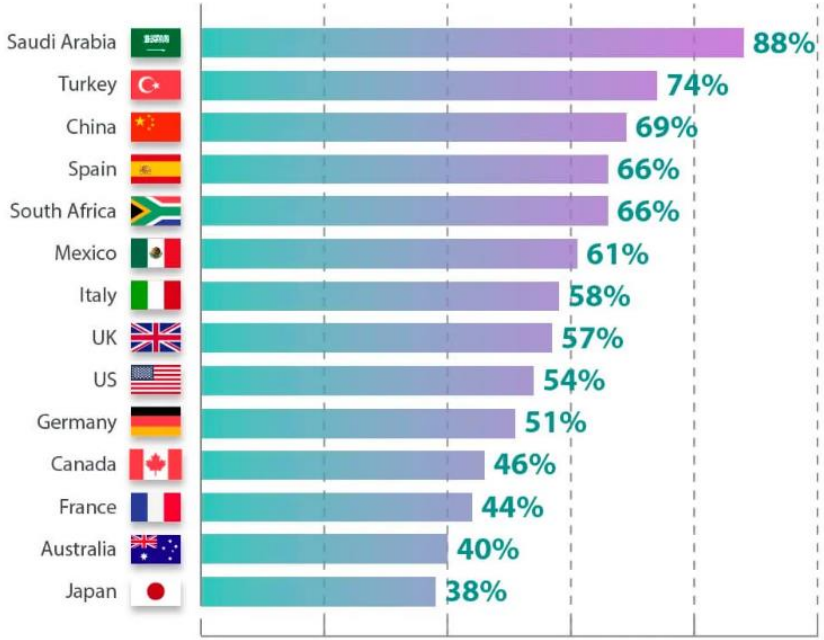
Knoxville Ransomware Attack Leads to IT Network Shutdown

The ransomware attack hit the Tennessee city of Knoxville this week, causing disruptions in various services.


THREATS
Vulnerability assessment and patch management
URL Filtering: to stop browser attacks
Exploit prevention
Cloud reputation analysis
Anti-malware engine scan
AI-based static analyzer
Data protection heuristics
Behavioral monitoring
Acronis Cyber Protection security technologies
1. Legitimate process injection detection
2. ETW/AMSI event analysis
3. Critical process protection
Critical areas scan to Fileless threats

It’s a worldwide problem! Everyone needs a solution

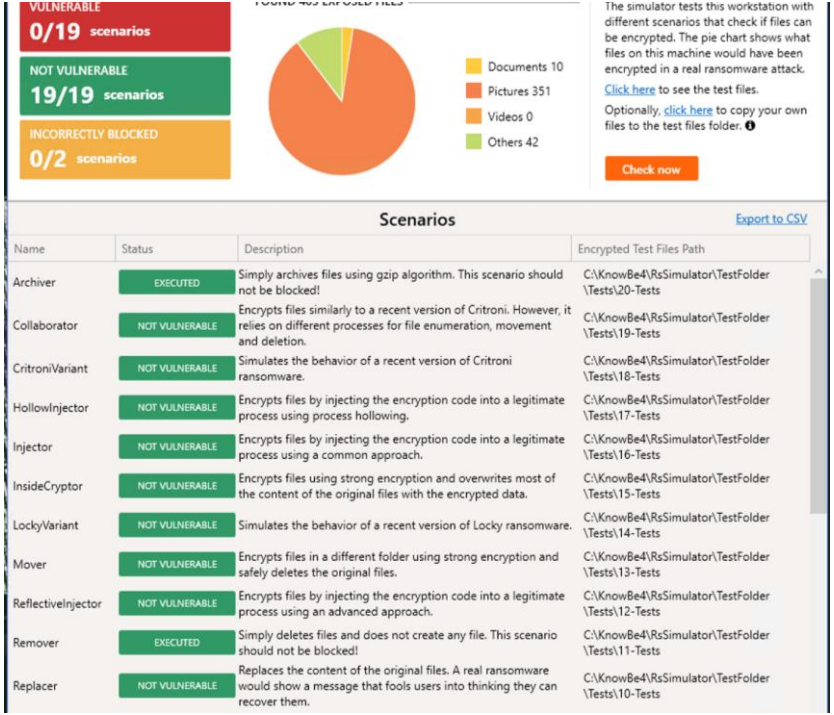
HOW MANY ORGANIZATIONS REPORTED RANSOM ATTACKS IN THE LAST YEAR?



Percentage of security professionals at medium and large organizations who responded that they were affected by ransomware within a 12 month period.

SafetyDetectives

Acronis Cyber Protect Cloud has perfect result in new version of RanSim



NOT VULNERABLE
19/19 scenarios

All 19 tests are passed (18 in some cases)

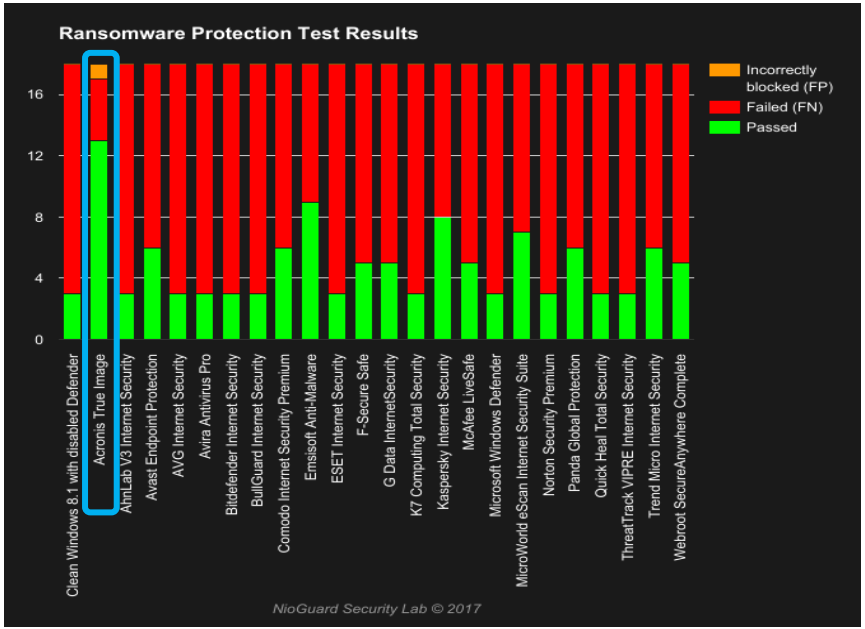
This is a result of Active Protection as well as other security engines in Acronis Cyber Protect Cloud

Tests emulate real ransomware strains like: Gandcrab, Pclock, Locky, Critoni, Chimera, XMRig, Fcrypt, CryptoLocker, Thor, Virlock, TeleCrypt and others.

Results on new version of RanSim (v. 2.1.0.3) released in April, 2020.

The first results of Acronis products in 2017

Almost all AV's are failing if ransomware(simulator) is allowed.
Means attack though scripts of trusted application will succeed.



The world's most famous hacker **Kevin Mitnick**

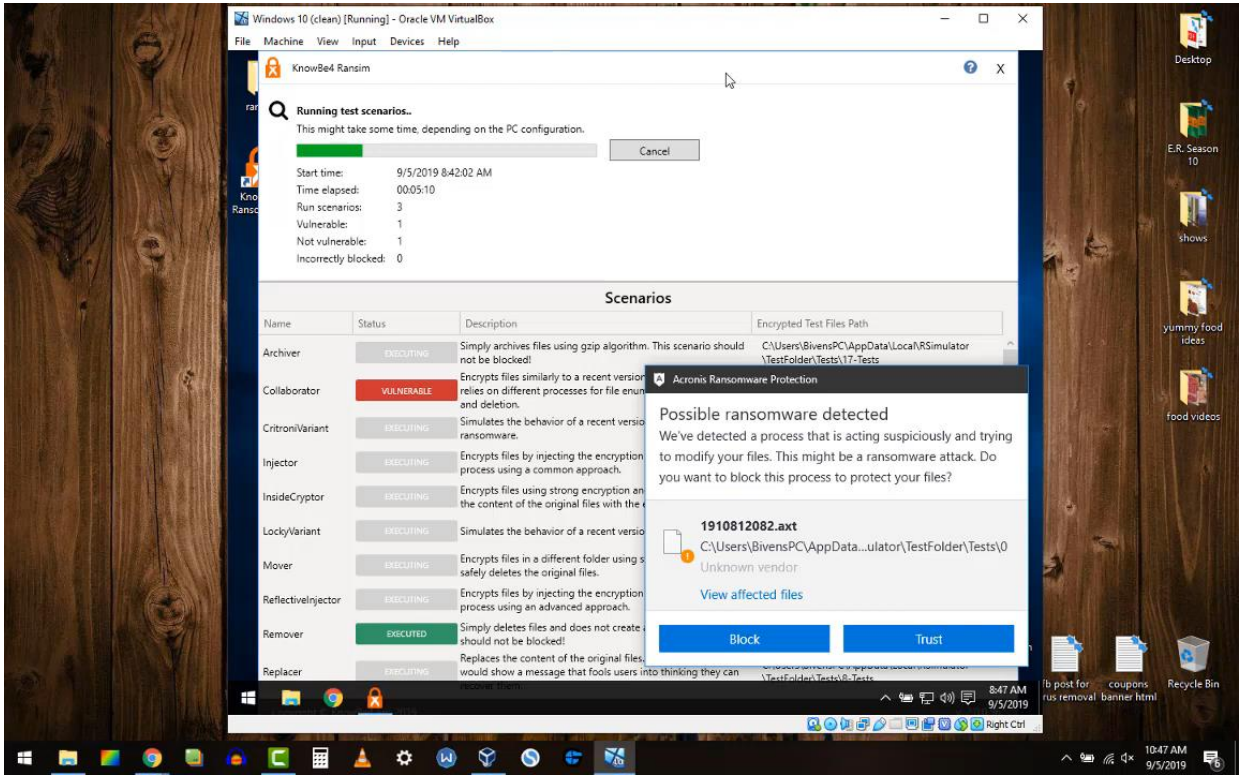
Top result in RanSim simulator

Acronis – 94% (15 out of 16)

Windows Defender – 12%

ESET – 0%

MalwareBytes – 77%



“Impressed by Acronis” external tester

WannaCry – blocked

Facebook Locker – blocked

…

Sodinokibi – blocked

Nemty - blocked

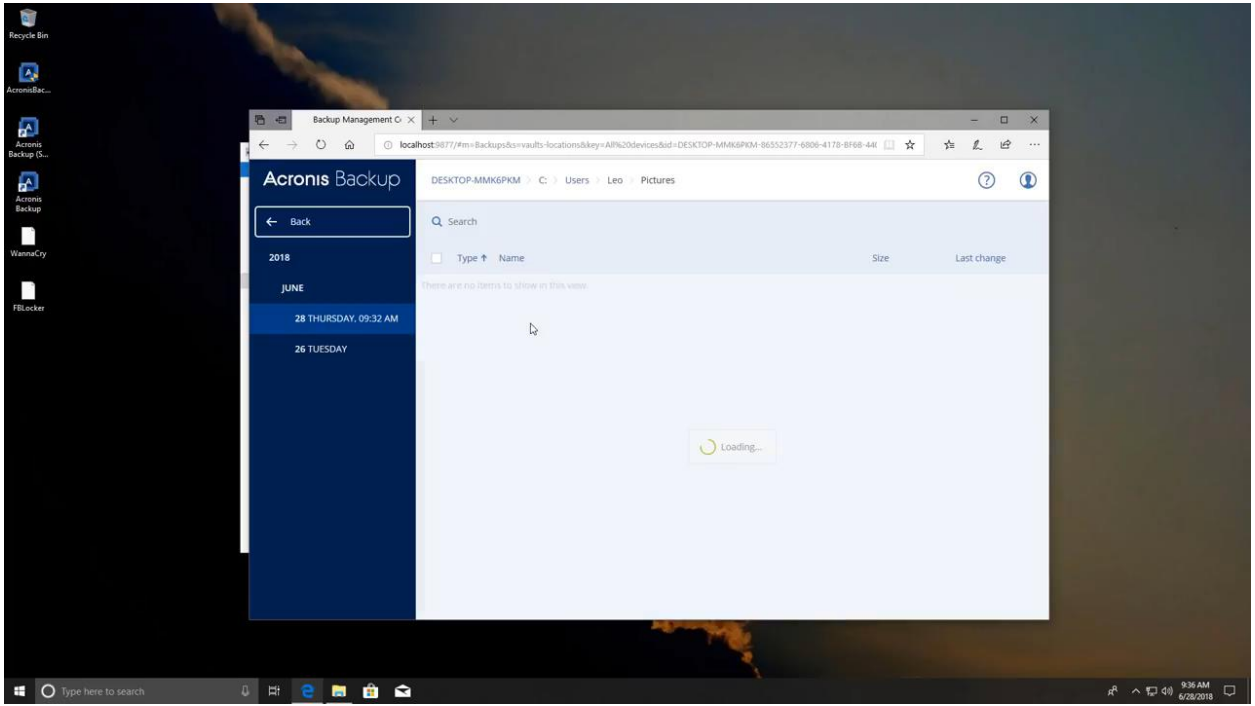
Maze - blocked

MegaCortex - blocked

FTCode - blocked

Phobos - blocked

Ruyk - blocked (!!!)



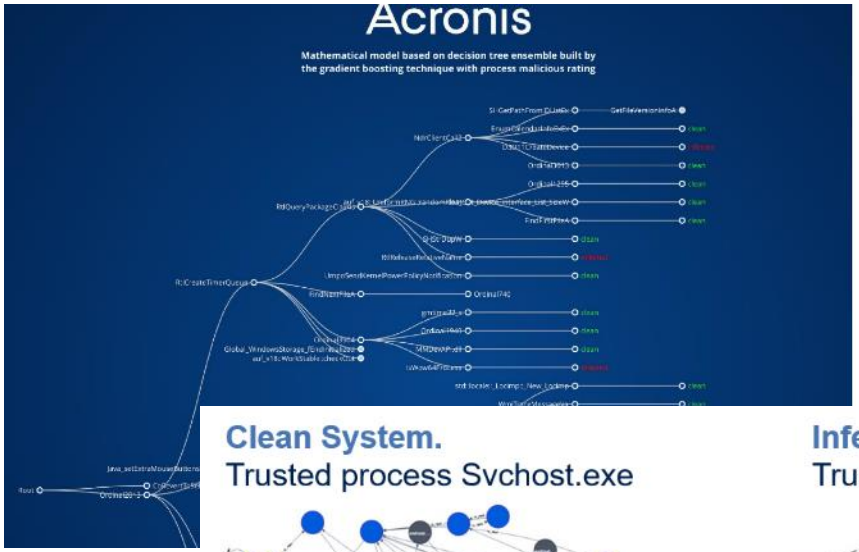
If there is any new ransomware – 99,9% chance that we detect it proactively

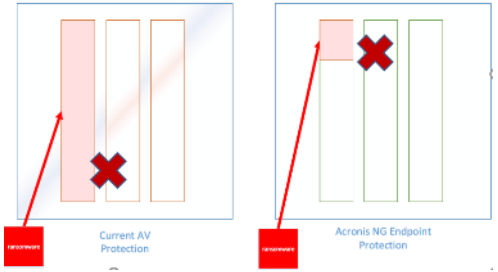
Acronis security industry recognition

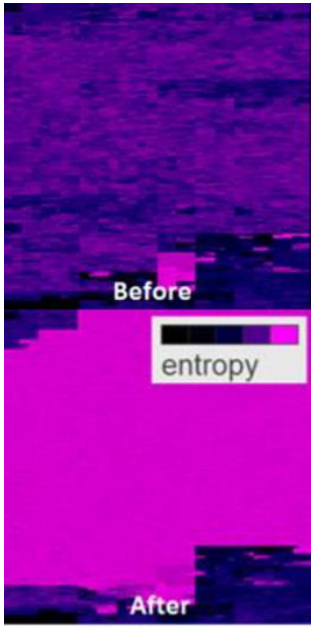
- MVI member
- VIRUSTOTAL member
- Cloud Security Alliance member
- Anti-Malware Testing Standard Organization member
- Anti-Phishing Working Group member
- MRG-Effitas participant and test winner
- AV-Comparatives participant
- VB100 certified
- AV-Test participant and test winner
- Anti-Malware Test Lab participant and test winner
- ICSA Labs participant
- NioGuard Security Lab participant and test winner

How? Technology leadership is a key!

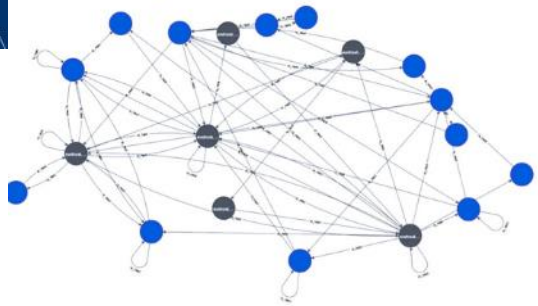
3. best protection from Ransomware, as we focus on it since 2015



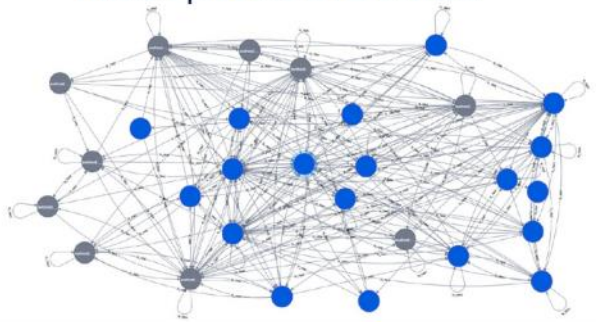




Clean System.
Trusted process Svchost.exe



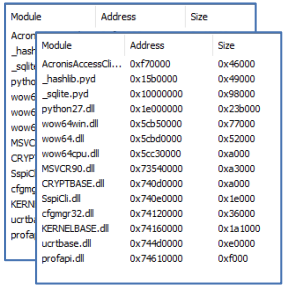
Infected System.
Trusted process Svchost.exe



How? No magic, just computer science

3. best protection from Ransomware, as we focus on it since 2015

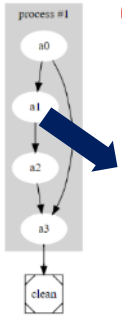
Clean processes



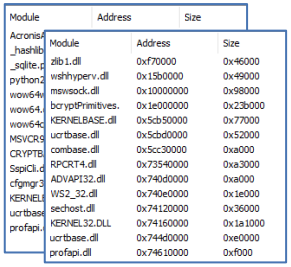
1

Data transformation

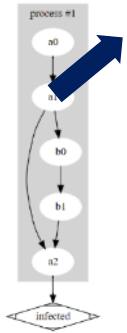
2



Infected processes



Data transformation



Training dataset

ntkrnlpa.exe,ntdll.dll,KernelBase.dll,mscorlib.ni.dll, …, **clean**
KernelBase.dll,kernel32.dll,kernel32.dll,ntdll.dll, …, **clean**
NetSetupSvc.dll,ELSCore.dll,ELSCore.dll, ,…,**clean**
com.docker.9pdb.exe, n/a,cryptsp.dll, …, **infected**
ntkrnlpa.exe,ntdll.dll,KernelBase.dll,mscorlib.ni.dll, **clean**

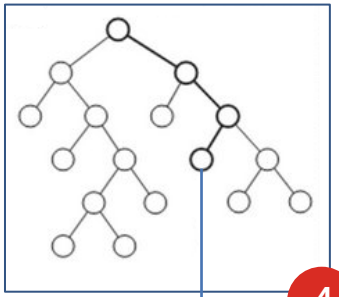
…
…
…

ntkrnlpa.exe,ntdll.dll,KernelBase.dll,mscorlib.ni.dll, **clean**
n/a,clr.dll,clr.dll,clr.dll, combase.dll,rpcrt4.dll, …, **clean**

3

Gradient Boosting Tree

Model: Decision Tree



4

Infected!!

1. Stack-traces collected from hundreds of clean and infected systems
2. More than 100M events related to data modification combined into a training dataset
3. Random tree model is trained. Resulting model size is 15 MB, compressed 1 MB
4. Decision made by average voting of random trees analyzing the sequence of stack frames and modules. Average accuracy is 99.95%, execution time 1-2 ms.

Systematic protection against modern techniques

2010	2014	2014	2016	2016	2016	2017-18
Detection of non-signed files	Exclude know legitimate system files	Protection for Windows only	Detection in running Windows system	Detection of executable files	Detection by checking file type/header	Use of Backup to protect against Ransomware
Malware signed by stolen certificate	Injects into system processes and acts on their behalf	Attacks Mac OS X and Linux	Infects before Windows starts	Uses scripts and non-malicious executables	Only body of the file is encrypted	Attacks & Encrypts different backup files
Compromised signatures check	Checks for injections in system processes (with Machine Learning)	Protection Windows, Mac and Linux	Pre-Boot anti-ransomware protection	Both executable and scripts detection	Entropy measurement	Acronis Active Protection™
Acronis	Acronis	Acronis	Acronis	Acronis	Acronis	

Preventing False Positives

Independent test results

- VB100 = 0 FPs
- AvComparatives = 0 FPs
- AvTest = 0 FPs
- ML model performance: 0.0005 false positives on 5M+ samples dataset

How we prevent false positives

- Cloud based Whitelisting services (3rd party and internal)
- Corporate **Whitelist from Backups**
- **Global Whitelist - external sources** of clean software (crawling of software aggregators, crawling of app stores)
- Telemetry analysis and **Cloud responses** for rapid resolution
- Digital Signature analysis and **discredited certificates database** maintenance
- Infrastructure **sandboxing to make avoid behavioral false positives**
- Infrastructure for **intensive testing of definitions before release**

Behavior Engine Rules - Trickbot

```
if ($cmdline =~ r/.*\\Windows\\system32\\cmd.exe \/c  \"\".*\\Users\\Public\\[a-zA-Z0-9]{3,32}\\[a-zA-Z0-9]{3,32}\.bat\" \"/i)
{

    if ($parent_cmdline == "" )
    {
     call(&get_process_info, query_puid = $parent_process_uid, cmdline = &parent_cmdline);
    }
    if ($parent_is_winword != 1 and
        $parent_cmdline =~ r/.*\\WINWORD.EXE/i)
    {
     $parent_is_winword := 1;
    }
    if ($starts_PS_downloader != 1 and
        .event_type == "si_create_process" and
        .cmdline =~ r/powershell.*\(New\-Object Net\.WebClient\)\.DownloadFile\('[^']+',\s+'.+\..*e.*x.*e'\)/i)
    {
     $starts_PS_downloader := 1;
    }
    if ($is_alert_raised_dotma != 1 and
        $starts_PS_downloader == 1 and
        $parent_is_winword == 1)
    {
      call(RaiseAlert, threat = "Downloader.TrickBot.Macro.A", rule=0);
    }

}
```

Behavior Engine Rules - Dridex

```
//Start stealing information
//Firt indicator of browser recon and stealer
if ($image_filename =~ r/\\windows\\(system32|SysWOW64)\\svchost\.exe/i and
    .event_type == "si_create_file" and
    .object_name =~ r/\\Device\\HarddiskVolume[0-9]\\Users\\.{2,32}\\AppData\\Local\\Microsoft\\Windows\\INetCache\\counters\.dat/i)
{
   $indicator_touch_1 := 1;
}
//second indicator of browser information stealer
if ($image_filename =~ r/\\windows\\(system32|SysWOW64)\\svchost\.exe/i and
   .event_type == "si_create_file" and
   .object_name =~ r/\\Device\\HarddiskVolume[0-9]\\Users\\.{2,32}\\AppData\\Local\\Microsoft\\Windows\\INetCookies/i) { $indicator_t
if ($image_filename =~ r/\\windows\\(system32|SysWOW64)\\svchost\.exe/i and
    .event_type == "si_create_file" and
    .object_name =~ r/\\Device\\HarddiskVolume[0-9]\\Users\\.{2,32}\\AppData\\Local\\Microsoft\\Windows\\History/i) { $indicator_touc

if ($is_alert_raised_mada != 1 and $indicator_touch_1 == 1 and $indicator_touch_2 == 1 and $indicator_touch_3 == 1)
{
   call(RaiseAlertParent, threat = "Malware.Dridex.A", rule=0);
}
```

Behavior Engine Rules – Riplace technique

```
rule Ransom_RIPlace_A
{

  if ( .event_type == "si_set_file_information" and
       .target_name == "" and
       .object_info.blob_type == 10 and
       .object_info.blob_size == 96 and
       .object_name =~ r/\.[a-zA-Z]{3,4}\.tmp$/i and
       .object_info.blob_dump =~ r/480000005c003f003f005c00/i)
    {
      if ($prev_file_name != .object_name)
      {
        $prev_file_name := .object_name;
        $replace_file_counter += 1;
        if ($is_alert_raised_rara != 1 and $replace_file_counter >= 10)
        {
          $is_alert_raised_rara := 1;
          call(RaiseAlert, threat="Ransom.RIPlace.A", rule=0);
        }
      }
    }
}
```

https://www.nyotron.com/collateral/RIPlace-report_compressed-3.pdf

Behavior Engine Rules – Event Types

Kernel level events

- si_create_file
- si_create_named_pipe
- si_set_file_information
- si_close_file
- si_read_file
- si_write_file
- si_create_key
- si_set_value_key
- si_create_process
- si_terminate_process
- si_load_image
- si_create_thread

Event Tracing for Windows

providers:

- &Microsoft-Windows-DNS-Client
  guid : 1C95126E-7EEA-49A9-A3FE-A378B03DDB4D
- &Microsoft-Windows-Kernel-Network
  guid : 7DD42A49-5329-4832-8DFD-43D979153A88
- &Microsoft-Windows-TCPIP
  guid : 2F07E2EE-15DB-40F1-90EF-9D7BA282188A
- &Microsoft-Windows-WinINet
  guid : 43D1A55C-76D6-4F7E-995C-64C711E5CAFE

events:

- name : etw_tcp_send_ipv4
  provider : *Microsoft-Windows-Kernel-Network
  …..

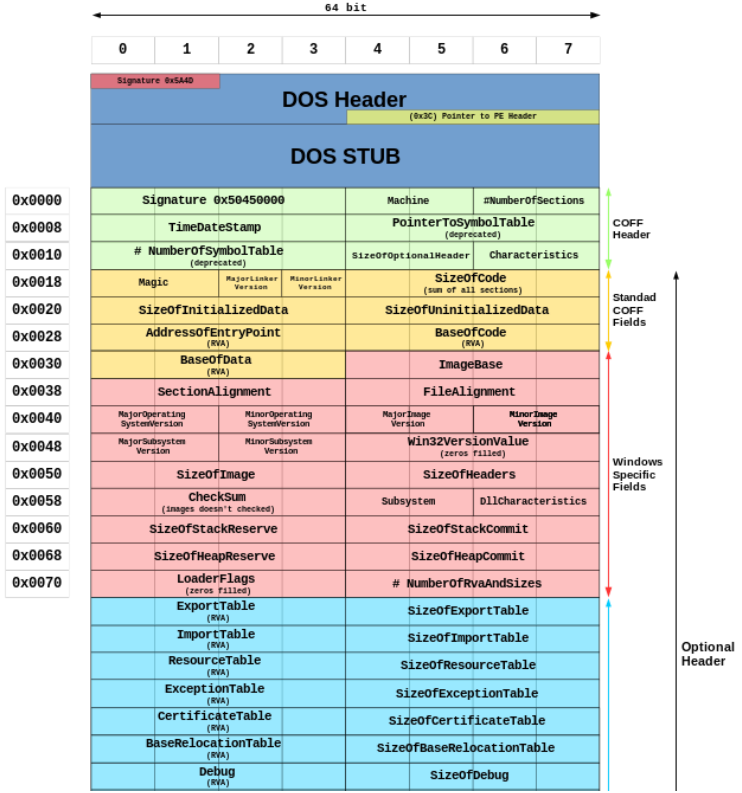
Comprehensive threat model under the hood

Behavior type	Details	Protection technique
File's overwrite in-place	Ransomware opens and modifies data files in-place	Driver provides file access notifications to the service with heuristics data, performs copy-on-write of suspicious activities. The service detects the case, suspends ransomware, the driver rolls back the file from its own cache.
File rename	Ransomware opens, renames and modifies data files	
New file creation	Ransomware creates a new file, copies original content, modifies a new file, deletes the original file.	
Master Boot Record overwrite	Ransomware opens PhysicalDrive, overwrites MBR, the system is rebooted, HDD/MFT is encrypted on reboot (chkdsk disguised)	The driver watches WRITE/SCSI operations to MBR via RAW FS, notifies the service, the service verifies the process and makes the decision.
Modification via file mapping	Ransomware opens the file, creates file mapping, modifies the file via mapping.	Data heuristics and copy-on-write
In-place overwrite/or rename/or new file with injection into known good processes	Ransomware makes the injection into a well known good process and does malicious actions as described above.	The driver provides injection attempts notifications to the service and the service instructs the driver to start watching the process without doing copy-on-write. If suspicious patterns are noticed, a user can be instructed to recover files from the cloud.
Master Boot Record overwriting + injection into known good processes	Ransomware makes the injection into a well known good process, overwrites MBR, the system is rebooted, HDD/MFT is encrypted on reboot (chkdsk disguised)	There are no known types of ransomware of this type so far, it can be possible to handle this only by constructing the list of processes, authorized to modify MBR.

AI-based static analysis of executable files

- Create portrait of the file based on static characteristics
- Advantages vs signature approach:
  - Allow **blocking** exe-files on pre-execution stage
  - **Doesn't** require regular **update** of ML model
  - Much smaller size of the model compare to AV bases
  - Fast response time: ~30 ms
  - Comparable detection rate

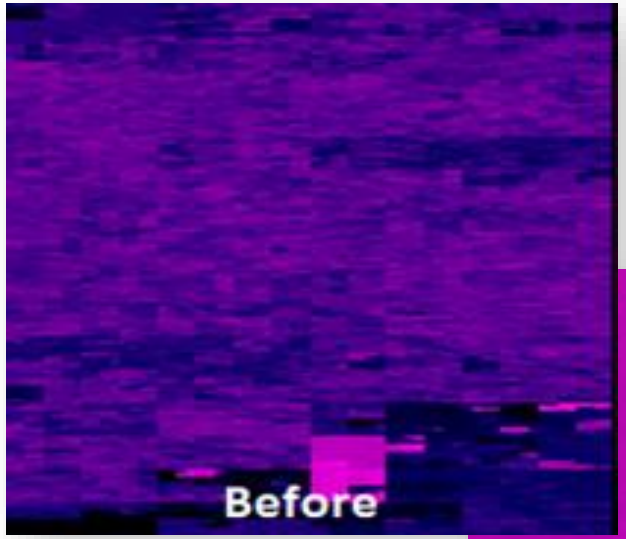
This scanner is working on VirusTotal from 2019



Data entropy analysis

Statistical distribution test
Compares data distribution within files to detect anomalies

Protection against injections
Detects ransomware that tries to partially encrypt files (Cerber) on behalf of trusted processes



Cyber protection front line: RYUK

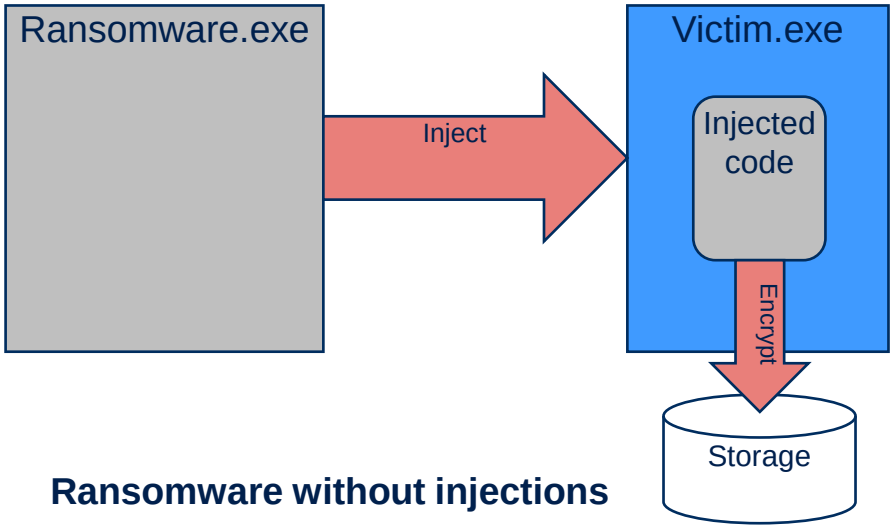
RYUK is actively targeting public establishments and govt. organizations in **United States** with ransom demand ranging into … of dollars.

Since March, Ryuk has collected:
1. $100,000 from the **public school** district in Rockville Centre, New York.
2. $130,000 from LaPorte County, Indiana
3. $490,000 from Lake City, Florida
4. $600,000 from Riviera Beach, Florida
5. $400,000 from rural Jackson County, Georgia

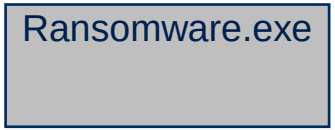
In July 2019, Ryuk infected Massachusetts city and demanded $5.3M in ransom which went under negotiation to pay $400K. It's only just for 4% percent of the city government's computers (!). Servers were recovered from backups/replacing during 2 months.
…"*New Bedford's IT staff have rebuilt the city's server network and implemented new security tools such as endpoint protection software*"

RYUK power: multi target injections!

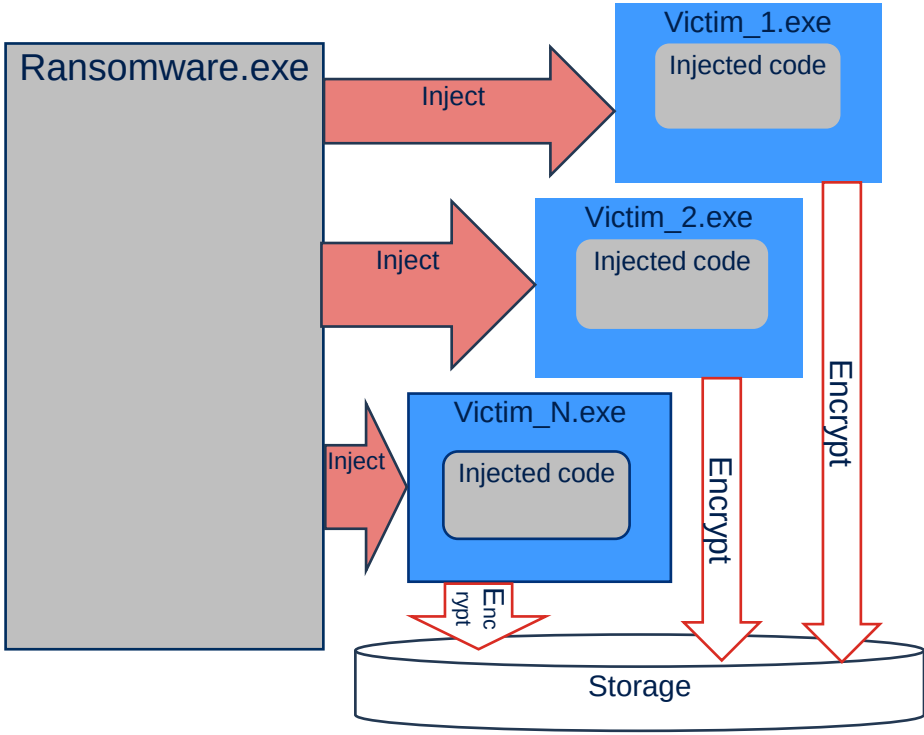
Ransomware with SINGLE TARGET injections



Ransomware without injections



Ransomware with MULTI TARGET injections



Anti-Cryptojacking, August 2019

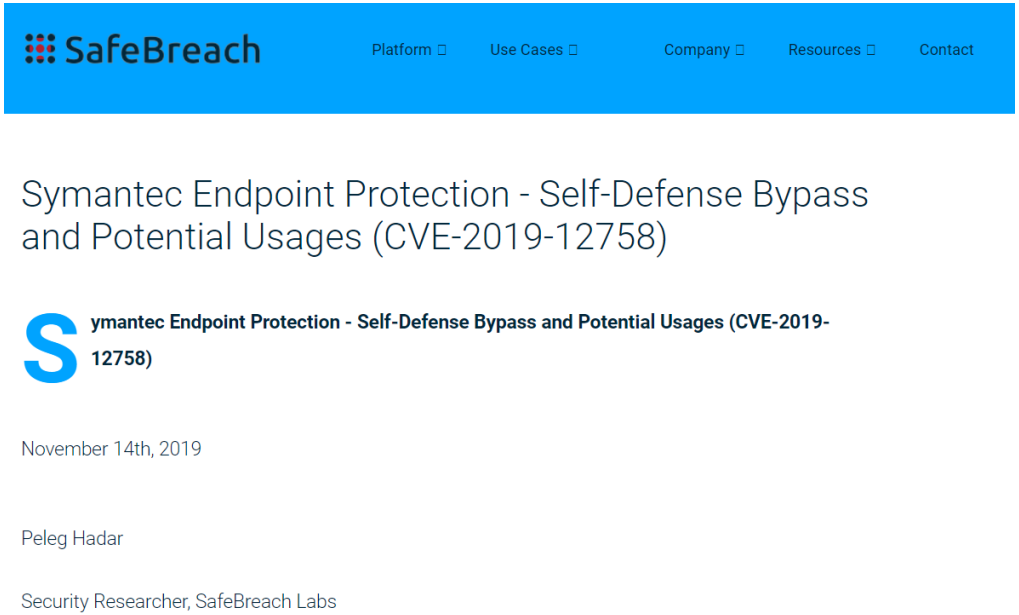
Product	False Positive Rate	Protection Rating	Protection Rating, %	Accuracy	Protection Class[1]
Acronis Backup	0%	68	94%	95%	AAA
Kaspersky Endpoint Security	0%	16	22%	28%	Not Passed
Symantec Endpoint Protection	0%	70	97%	97%	AAA
Bitdefender GravityZone Security for Endpoints	0%	54	75%	77%	A
ESET Endpoint Security	0%	68	94%	95%	AAA
McAfee Endpoint Security	0%	53	74%	77%	A
Avira Antivirus Pro - Business Edition	0%	56	78%	79%	A
Avast Business Antivirus Pro Plus	0%	50	69%	72%	A
F-Secure Business Suite	0%	59	82%	85%	AA

https://www.nioguard.com/2019/08/anti-cryptojacking-test-july-2019.html

Unbeatable backups with security self-defense

1. Number of ransomware families that are trying to stop security and backup agents is growing.
2. Discovered in August 2019, HILDACRYPT ransomware specifically targets backup and anti-virus solutions from vendors including Veeam, Symantec, Veritas, Carbonite, Sophos, McAfee, ESET and others: more than 100 services are disabled, 337 file types are encrypted.
3. HILDACRYPT can easily stop Veritas and Veeam backup solutions, any kind of data restoration is unlikely to be successful after this attack (prove link).
4. Acronis is resistant to HILDACRYPT attack thanks to most powerful in the industry Self-Defense module.
5. It's proven by Acronis total domination in 31-simulating attacks test (prove link) with **87%** vs 15% averaging for Arcserve, Veeam and Veritas. Malware is trying to
   a) delete backup files and registry records,
   b) stop product's files, processes, services;
   c) inject malicious code into a backup agent and act on behalf of a backup solution gaining all necessary privileges to control backup files.

Self-defense is not easy even for top vendors



Acronis unlike Symantec has a proper implementation of ELAM driver.

Acronis created its own ELAM driver for its cyber protection products and uses this driver for the AM-PPL protection of the Acronis Cyber Protect Cloud service.

Acronis' ELAM driver allows listing of the specific certificate hashes that are used to allow or deny a dynamic library from loading as a PPL protected process.

Independent evaluation of self-defense power

Product name	Platform 32-bit / 64-bit	The number of passed tests	The number of failed tests	Not applicable (N/A)	Pass rate
Acronis Backup	32	26	4	1	87%
	64	25	6	0	81%
Arcserve	32	5	24	2	17%
	64	4	26		
Veeam	32	4	26		
	64	4	27		
Veritas Backup Exec	32	5	22		
	64	4	27		

https://www.acronis.com/en-us/blog/posts/independently-proven-acronis-backups-self-defense-delivers-unmatched-protection-corporate-data

PRODUCT	AWARD	POINTS (OUT OF 35)	% PASSED
Acronis True Image	Gold Self-Protection Award	29	83%
EaseUS ToDo Backup Free	Bronze Self-Protection Award	11	28%
Carbonite Home		10	26%
Macrium Reflect Home Edition		10	26%
NovaBackup PC	FAILED TEST	9	23%
CrashPlan Free		8	21%
iDrive		7	18%

https://www.acronis.com/en-us/blog/posts/popular-backup-solutions-easily-disabled-recent-hildacrypt-ransomware

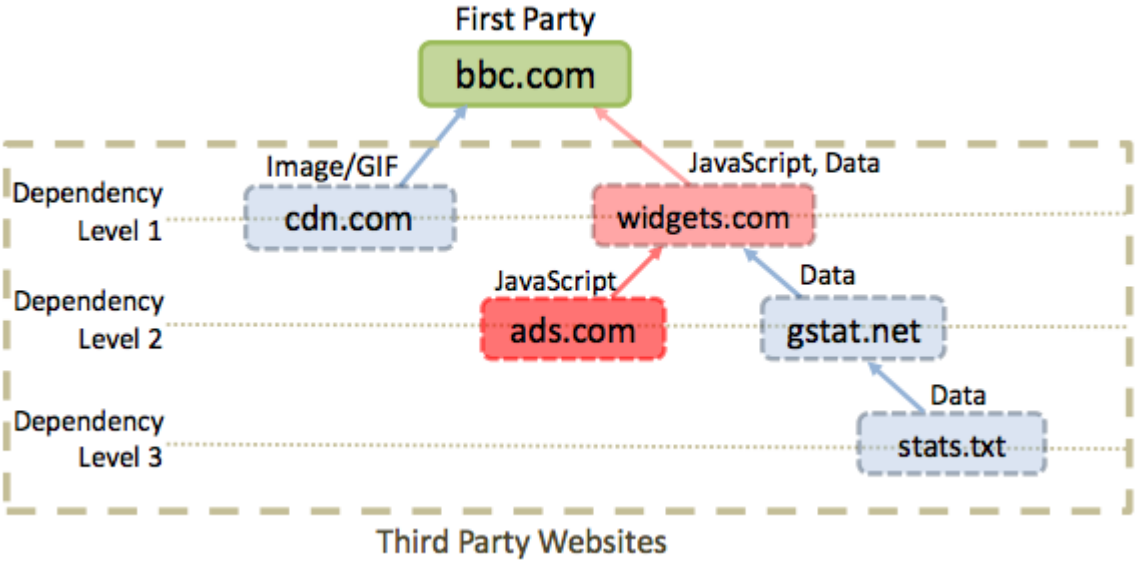
Malicious URLs

Worldwide, over 56% of the population has access to the internet. That's 3.2 billion people

It's estimated that up to 18.5 million websites are infected with malicious content

Hackers are incredibly clever and they're even more deceptive. That's why they design malicious websites to look as genuine as possible.

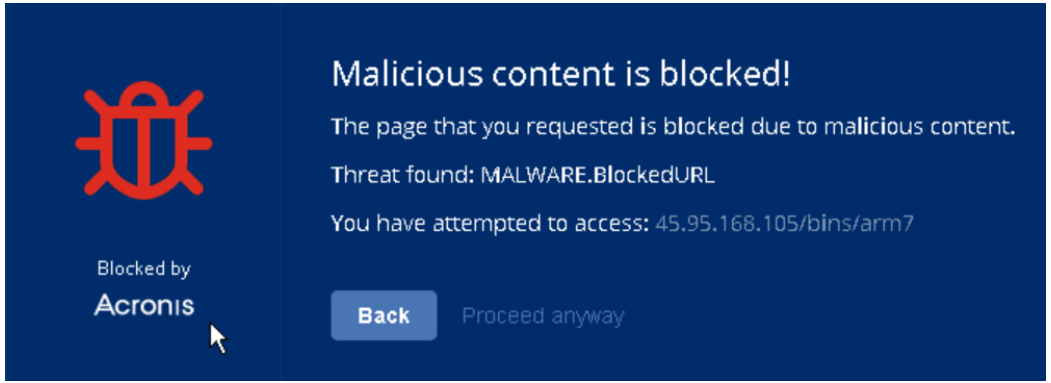
We, as humans, make quick decisions based on first impressions and, in this busy digital age, this is never truer than when online.

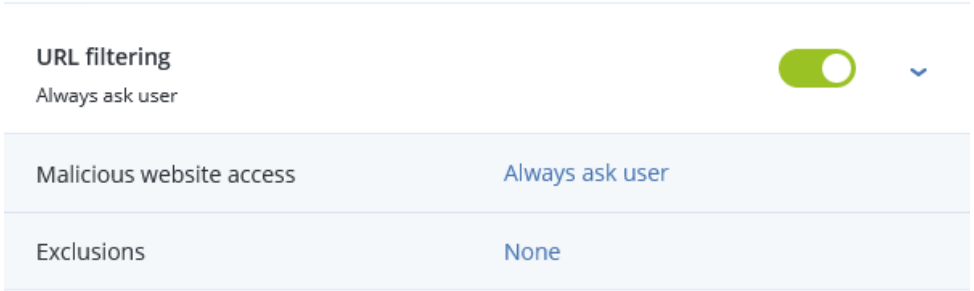


Example of a dependency chain to import external resources, including ad providers, tracking and analytics services, CDNs and potentially malicious

Acronis Malicious URLs filtering

3. best protection from Ransomware, as we focus on it since 2015



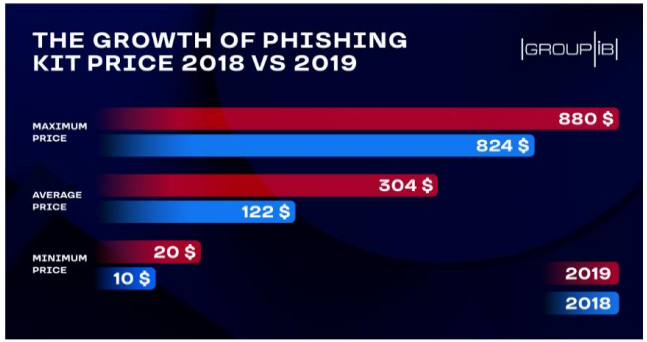


Acronis Anti-Phishing protection

Phishing kit prices skyrocketed in 2019 by 149%

The average price for a phishing kit in 2019 was $304, up from $122 recorded in 2018.

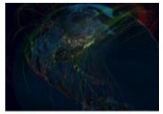
By Catalin Cimpanu for Zero Day | April 15, 2020 -- 09:00 GMT (17:00 GMT+08:00) | Topic: Security



MORE FROM CATALIN CIMPANU

Security
Microsoft: COVID-19 malware attacks were barely a blip in total malware volume

Security
Zoom backtracks and plans to offer end-to-end encryption to all users



Security
AWS said it mitigated a 2.3 Tbps DDoS attack, the largest ever

Securit
North K
hacker

Anti-phishing and Fraud Prevention

Blocking of Phishing URLs

- Intercept HTTP/HTTPs traffic on the endpoint
- NLP models and domain distance calculation (e.g. faceb00k.com)
- Collect phishing databases from 3rd parties (APGW, Netcraft, Spamhaus, Bitdefender)

Detection of phishing emails

- Content analysis for phishing email patterns (delivery notifications, password change notifications, voicemails, etc.)
- Ability to scan O365 and GSuite email backups

Detection of phishing websites

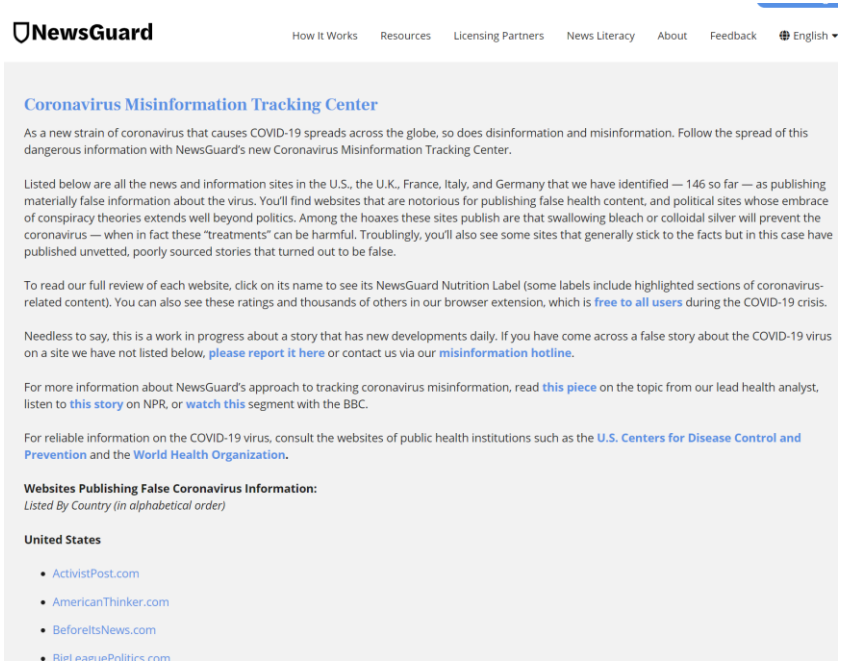
- Content analysis for phishing web pages (mimicking logon pages from real websites)

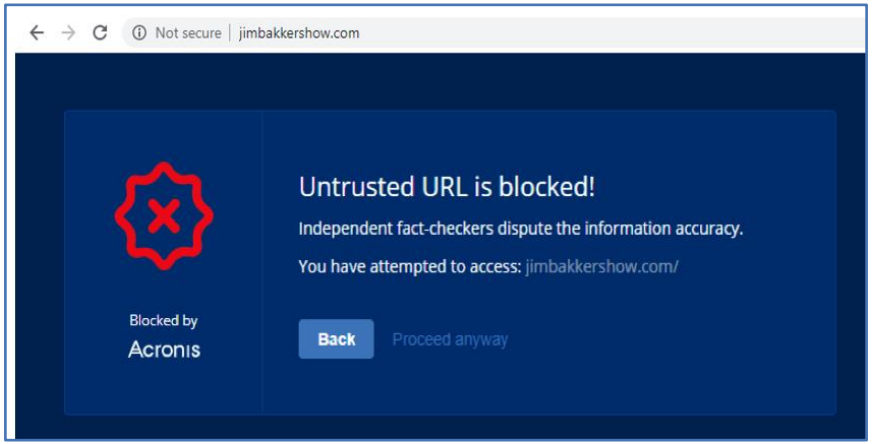
Mailbox anomaly detection to identify business email compromise

- Anomaly mailbox rules (e.g. forwarding)
- Sender reputation and communication patters/frequency

Covid-19 fake news sites blocking

Fact-checking by Acronis analysts and communities



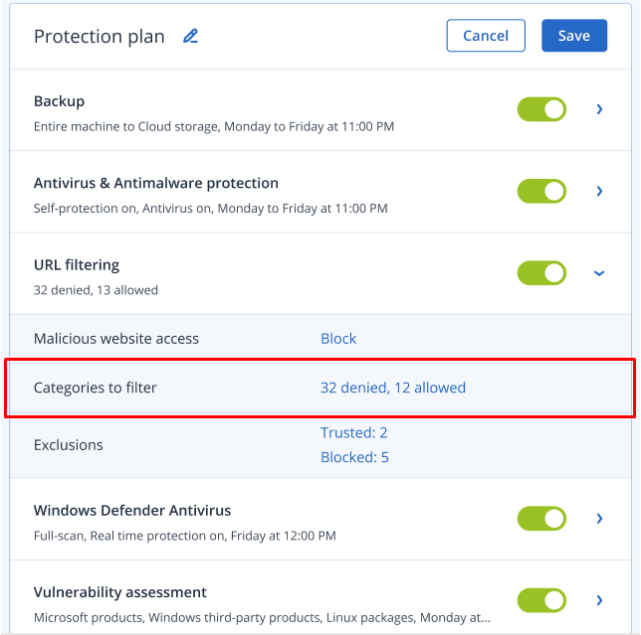


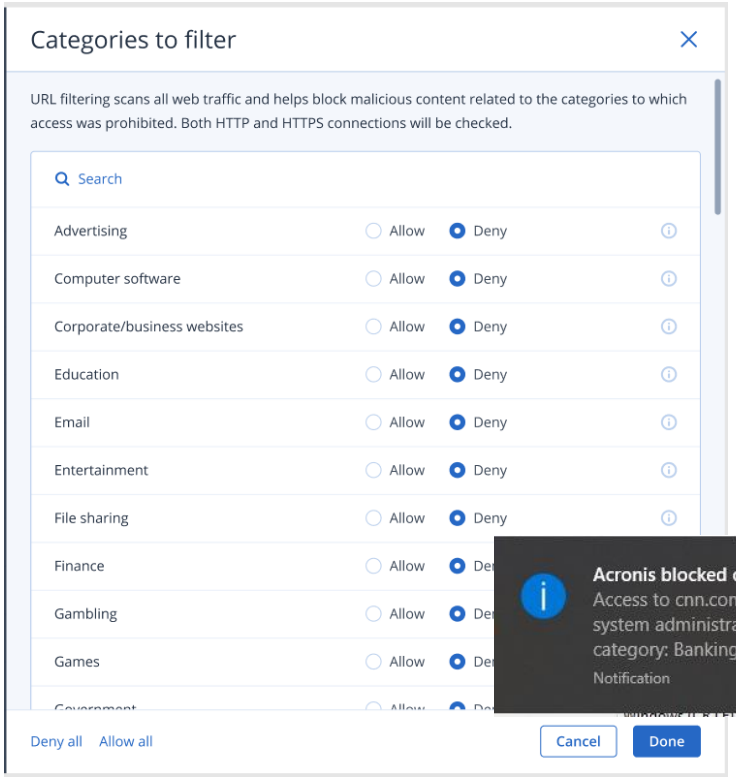
URLs Categorization (June update)

Ability to block 40+ web categories.

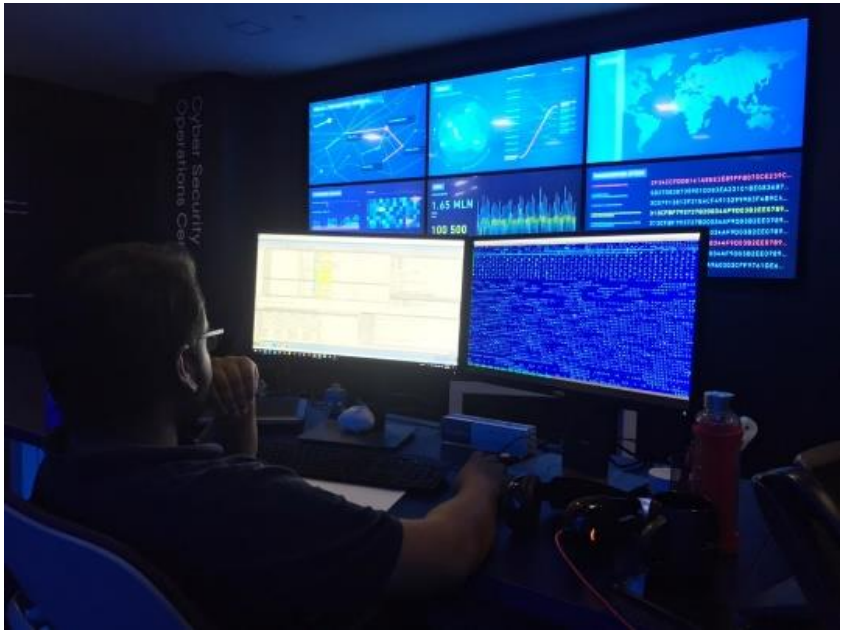
Support HTTP and most HTTPs websites.

New OS notifications informing that access was blocked.





Acronis Cyber Protection Operations Center:
Daily Acronis Intelligence



Follow-the-Sun:
1. Singapore (8 hours)
2. Switzerland (8 hours)
3. USA (8 hours)

24 x 7 support of Acronis Partners
and customers with new malware, vulnerabilities
and smart protection alerts

Why Acronis is an innovator in cyber protection

A lot of experience
- Best people from the industry
- A lot of cyber security experience
- Across various fields

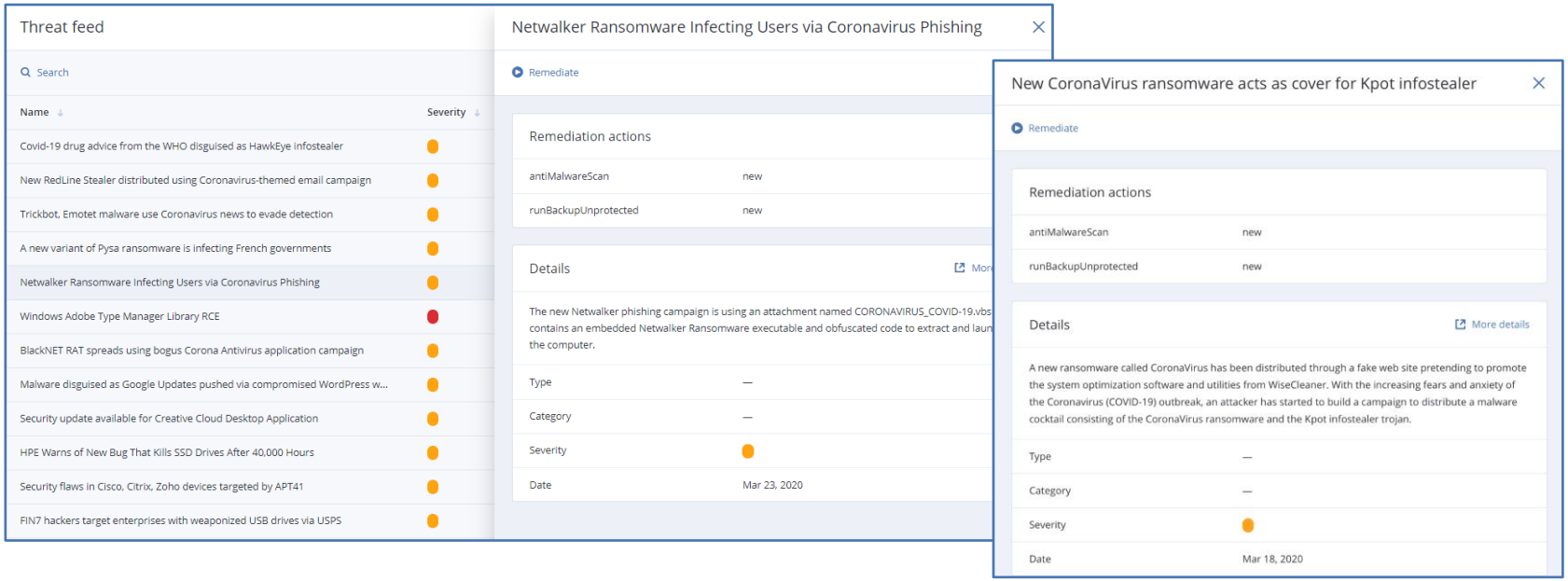
Fast innovator
- Agile company structure
- Large knowledge pool
- Fast development of innovation

Interdisciplinary
- Combining the best from each world
- Next-gen anti-malware, data protection
- and security management

Acronis hired top talents from various security companies

CPOCs alerts on COVID-19 related malware

Don’t let malware hide behind coronavirus news



Are you reading our blog's articles? Must!

3. best protection from Ransomware, as we focus on it since 2015

From deep malware research to expert opinion on incidents

16 Aug 2019

[Meet Buran: The New Delphi Ransomware Delivered via RIG Exploit Kit]

- Buran is a new version of the Vega ransomware strain (a.k.a. Jamper, Ghost, Buhtrap) that attacked accountants from February through April 2019.

11 Jul 2019

[Modular Cryptojackers Now Deliver Illicit Cryptomining to Cover Multiple Platforms at Once]

- Cryptojacking attacks are not going away any time soon. Instead, they're becoming more sophisticated – and more dangerous.

24 Jun 2019

[Ransomware Attack Costs $1.5 Million in Riviera Beach, FL]

- Ransomware continues to be a nightmare for individuals and businesses worldwide.

20 Jun 2019

[Cashing In on Crime: GandCrab May End, But The Threat of Ransomware Continues]

- They say crime doesn't pay, but clearly the architects behind GandCrab ransomware didn't get that memo.

13 Jun 2019

[Ransomware Crushes Another Manufacturing Industry Target]

- Another of the world's major manufacturers was laid low recently by a ransomware attack.

17 Jul 2019

[Taking Deep Dive into Sodinokibi Ransomware]

- While Sodinokibi ransomware has been in the news recently, technical details for that particular strain have been far less visible.

Acronis

#CyberFit

Power of integration

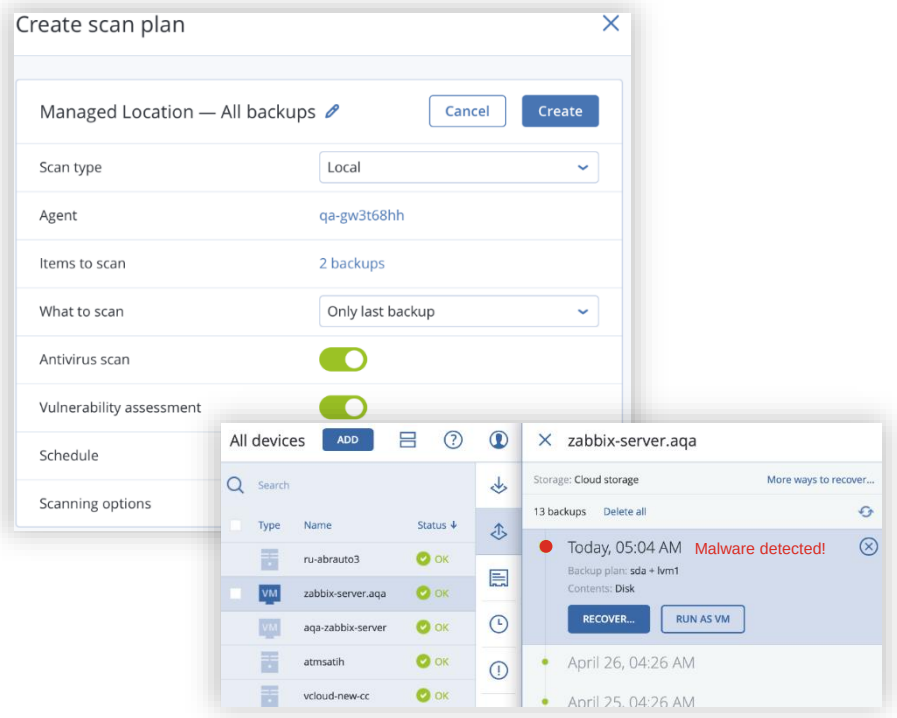
Malware Scan in Centralized Locations

4. decrease load on the network from antivirus scans

Anti-malware scanning and vulnerability assessments of backups - provide additional security

Scan of full disk backup at centralized location to find potential vulnerabilities and malware infections – ensures a user restores malware-free backup

- Increases potential of rootkits and bootkits detections
- Restore only clean data
- Reduces loads of client endpoints



Whitelists from backups

Build global and local whitelists to prevent false detections while making more aggressive, accurate heuristics

7. Become a real **proactive CISO:**

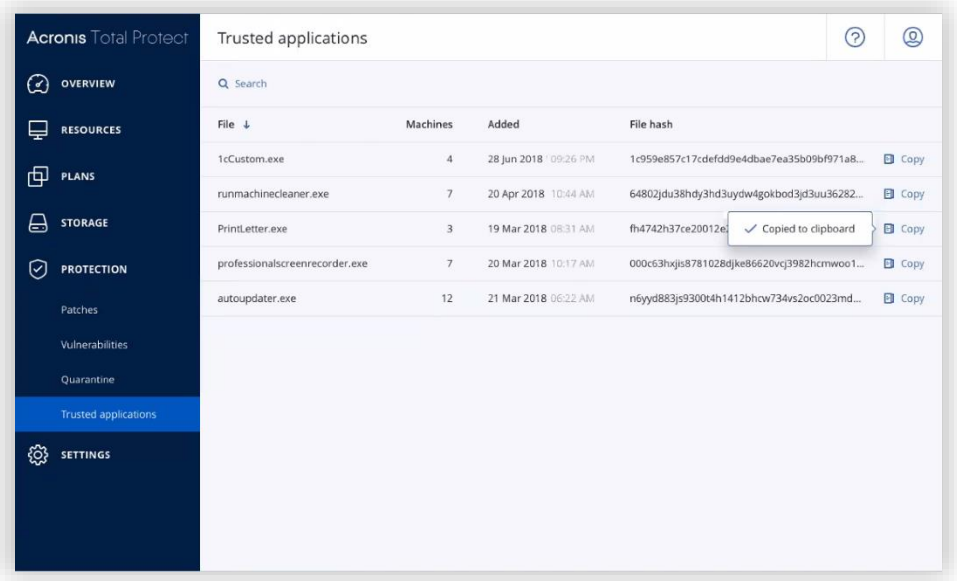
- extract value from backups to build company-specific whitelist

Traditional global whitelisting does not support custom applications.

Acronis Cyber Protect scan backups with anti-malware technologies to whitelist organizational unique apps and avoid “false positives” in the future

Specific rules of whitelisting are *not public* – in purpose: to prevent potential attacks on this feature

- Eliminates time-consuming manual whitelisting of unique apps
- Ensures greater productivity
- Improves detection rate via improved heuristics



Why? “False positives” can prevent access to data or apps. Automation saves time, improves protection

Continuous Data Protection (1/2)

1. unique capability to survive a potential attack without loss

Safe/Instant remediation without data loss: Close to Zero RPO

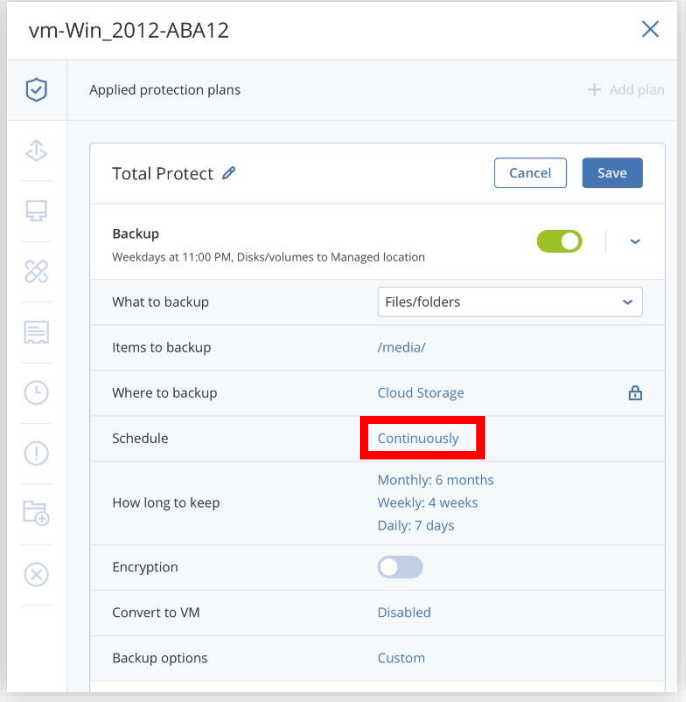
Define critical apps for every device that users are working with most often

Agent monitors every change made in list

In case of malware infection (or other loss)

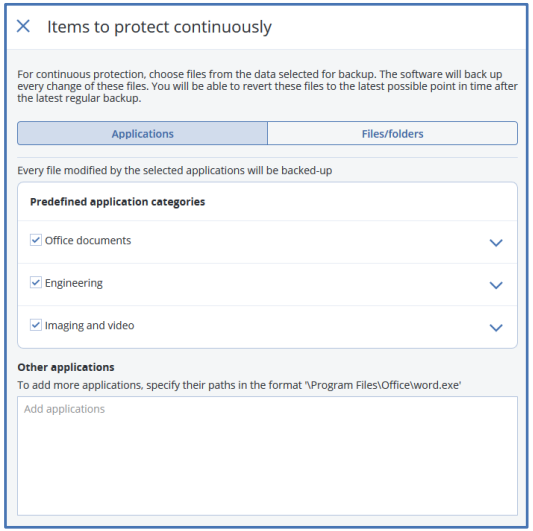
- Restore data from last backup
- Apply latest collected changes to the last backup
- No data lost.

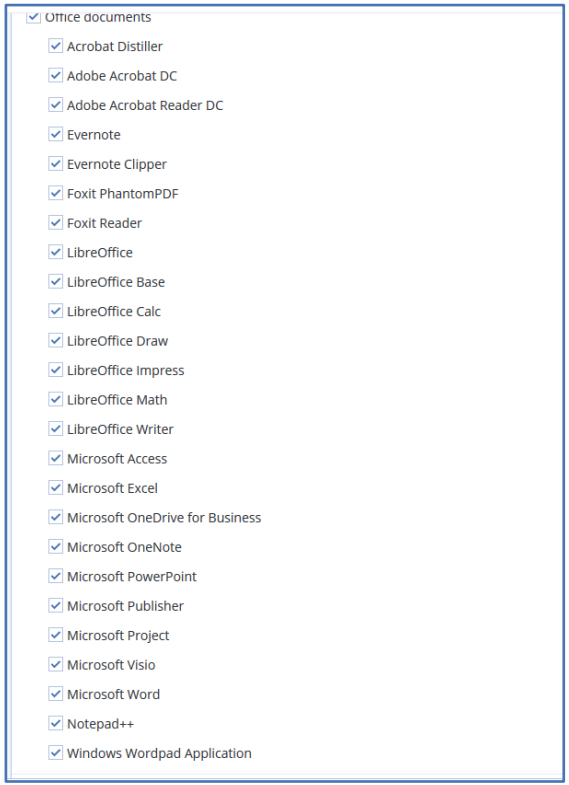
- Ensures users won't lose work in progress
- IT controls what is continuously backed up – Office documents, financial forms, logs, graphic files, etc.

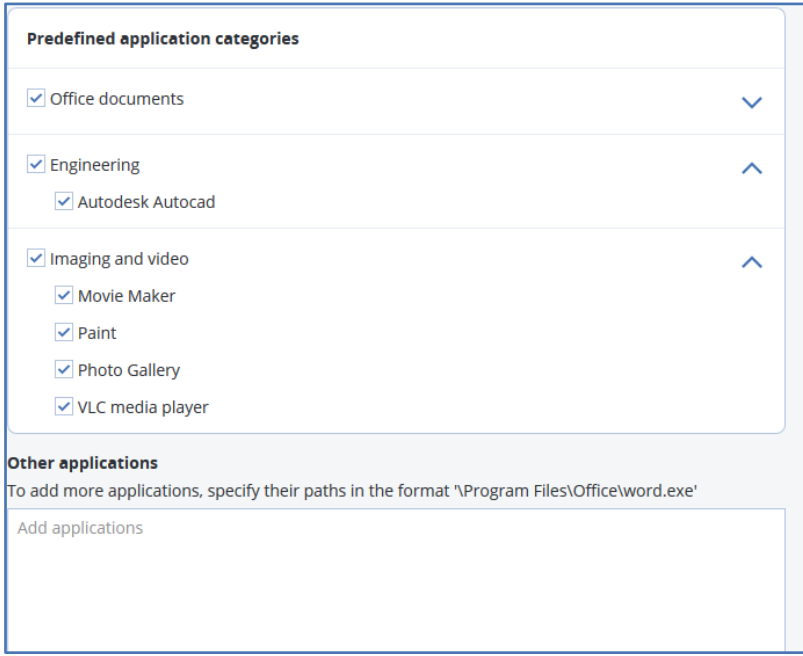


Continuous Data Protection (2/2)

1. unique capability to survive a potential attack without loss



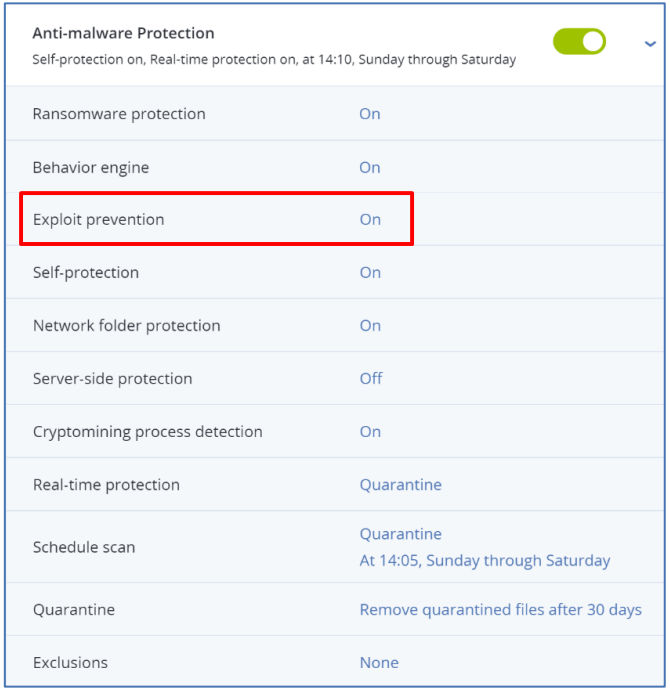




0-day Exploit Prevention (July update)

- Behavior Engine will be able to detect **exploitation attempts** in applications like MS Office, Adobe Reader, etc.

- Wide range of exploitation techniques:
  - Memory protection (e.g. Stack Pivot, Mandatory ASLR, Import Address Table Filtering)
  - Return-oriented programming (ROP) protection
  - Code injection protection (e.g. DLL Hijacking, Process Hollowing, Reflective DLL Injection)
  - Privilege escalation protection (e.g. Access token manipulation)



Acronis Cyber Protect 2H-2020

	Theme	Q3-2020	Q4-2020
1	Remote worker protection	• Run critical apps in a sandbox	• Endpoint firewall • Content-based Data Protection Map • USB device control
2	Lightweight RMM	• Remote Assistance mode • Software / Hardware inventory • Remote process / script execution	• Monitoring (CPU, RAM, HDD free space, etc.)
3	Feature parity all OSes	• Anti-Malware protection for Linux • Active Protection for macOS	• Vulnerability Assessment for Linux • Vulnerability Assessment for Mac • HDD health support on Linux, Mac
4	Third-party anti-viruses replacement	• Uninstallation protection • Improved file-less malware protection • URL filtering with categorization • Immediate email alert on malware detection • Exploit prevention	• Email security • App black/white listing • Exploit prevention • Autonomous engine with self-learning pre-execution analyzer
5	Existing features improvements	• Update interruption handling in patch mgmnt. • Extended metrics collection by Acronis CEP	• New apps support in third-party patching

Acronis

#CyberFit

Why Acronis Cybersecurity is better than competitors

Example of CrowdStrike

Ransomware protection	CS	A	CS + A
AI-based pre-execution detection			
Signature-based detection			
Behavior-based detection			
AI-based Injection-detection			
Entropy analysis			
Recovery from cached files changes			
Integrated recovery from backups			
Anti-tampering protection			
Processes killing			
Processes injections			
Critical files changes			
Critical registry records changes			
Services stop			
Uninstallation protection			
Anti-phishing protection			
URL filtering			
Real-time protection			
On-Execution			
On-Access			
send as mail attachment			
local copy to Dropbox or a file share			
remote upload to NAS and file shares			
Cryptominers protection			
CPU-based high usage detection			
GPU-based high usage detection			
Hidden windows detection			
Mining pool detection			

(1) Weak ransomware protection

Can result in data loss in the case of ransomware or wipers

Ryuk, LockerGoga and Cerber were not prevented and encrypted sensitive files with no prevention and no option for restoring them.

No behavioral blocks for any RanSim test cases

- Very basic behavior-based heuristics
- Full focus on ML detection with cloud focus
- New payload can bypass ML detection

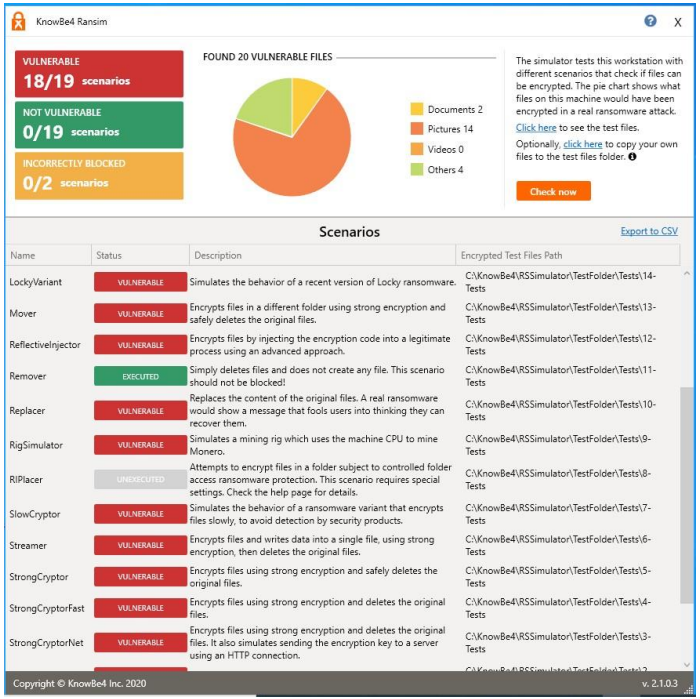
Acronis Cyber Protect

- Strong behavior detections against threats
- Entropy analysis combats advanced ransomware

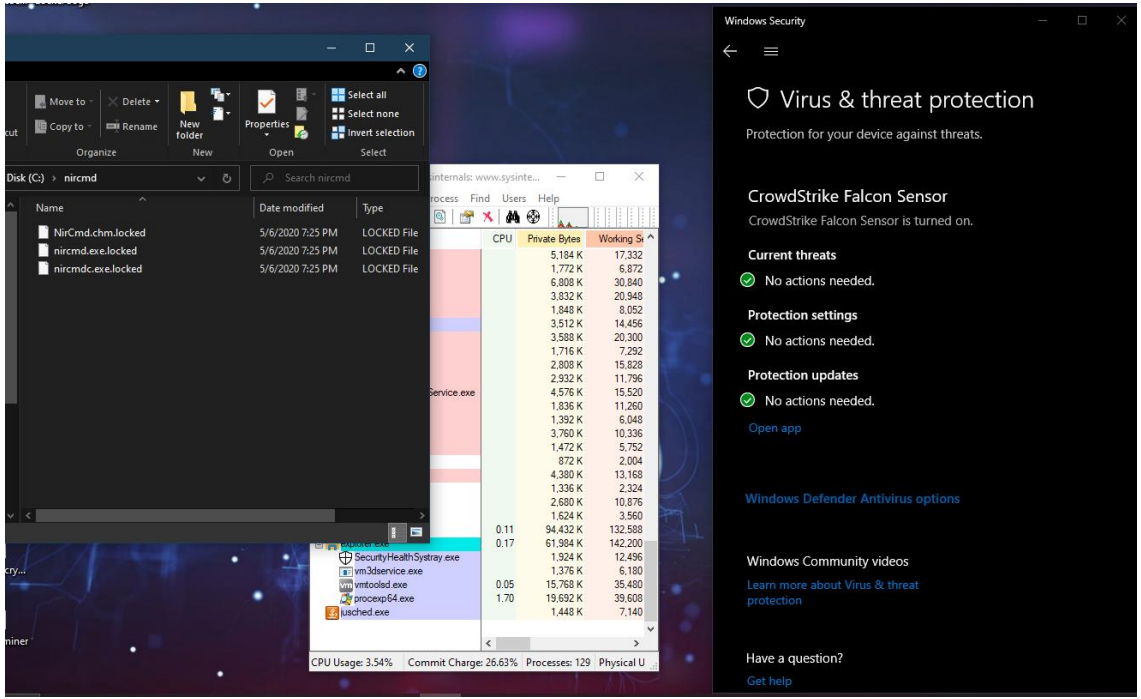
	CS	A
AI-based pre-execution detection		
Signature-based detection		
Behavior-based detection		
AI-based Injection-detection		
Entropy analysis		
Recovery from cached files changes		
Integrated recovery from backups		

(1) Weak Ransomware Protection

RanSim results – poor behavior analysis



Successful execution of LockerGoga ransomware



(2) Insufficient Anti-Tamper Protection

Can allow attackers to disable the protection

Attacker can remove CrowdStrike registry keys

Disables all protection and monitoring

Attack third-party applications e.g. Microsoft Teams

- Terminate Process With Remote Thread
- Terminate Process With Remote Thread Dll
- Terminate Process With Section Unmap

- Uses an AM-PPL (ELAM) driver to self-protect
- Unprotected files and registry keys
- Product can be disabled

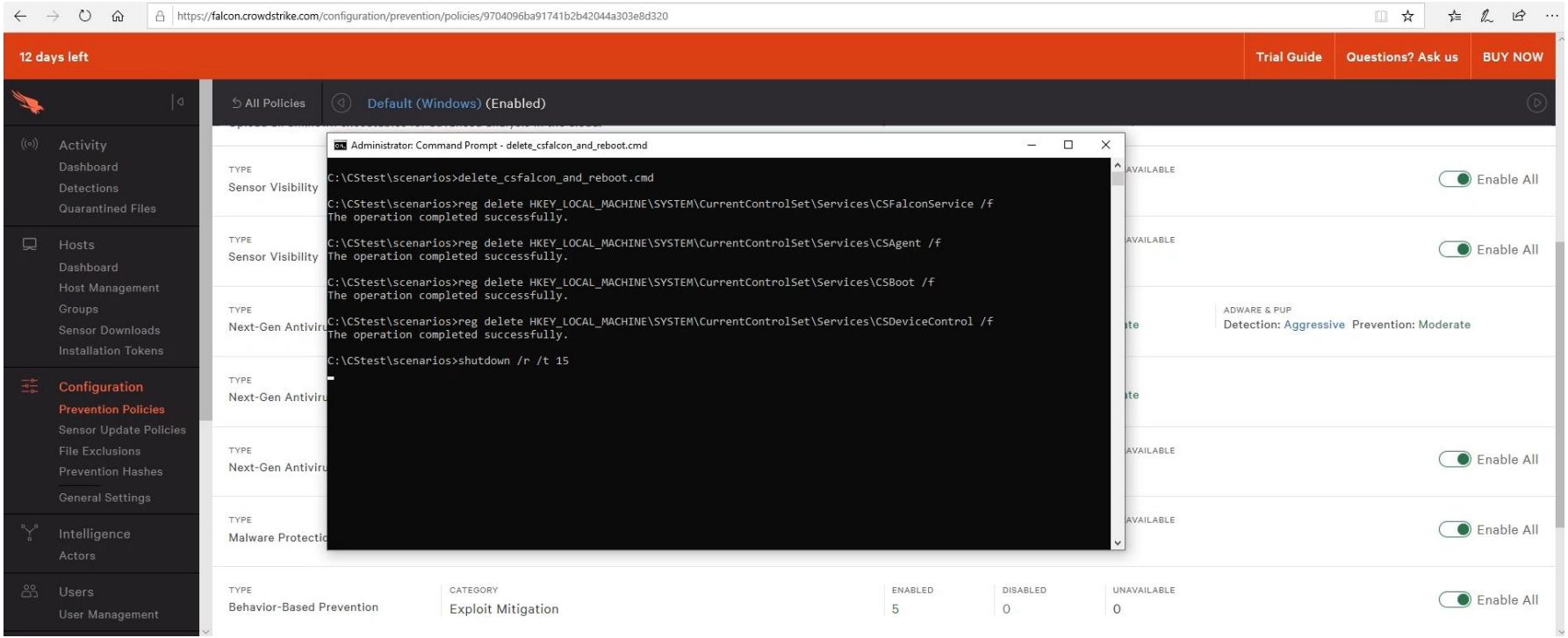
Acronis Cyber Protect

- Strong anti-tampering and self-protect feature
- Protection of third-party apps e.g. Microsoft Teams

	CS	A
Processes killing		
Processes injections		
Critical files changes		
Critical registry records changes		
Services stop		
Uninstallation protection		

(2) Insufficient Anti-Tamper Protection

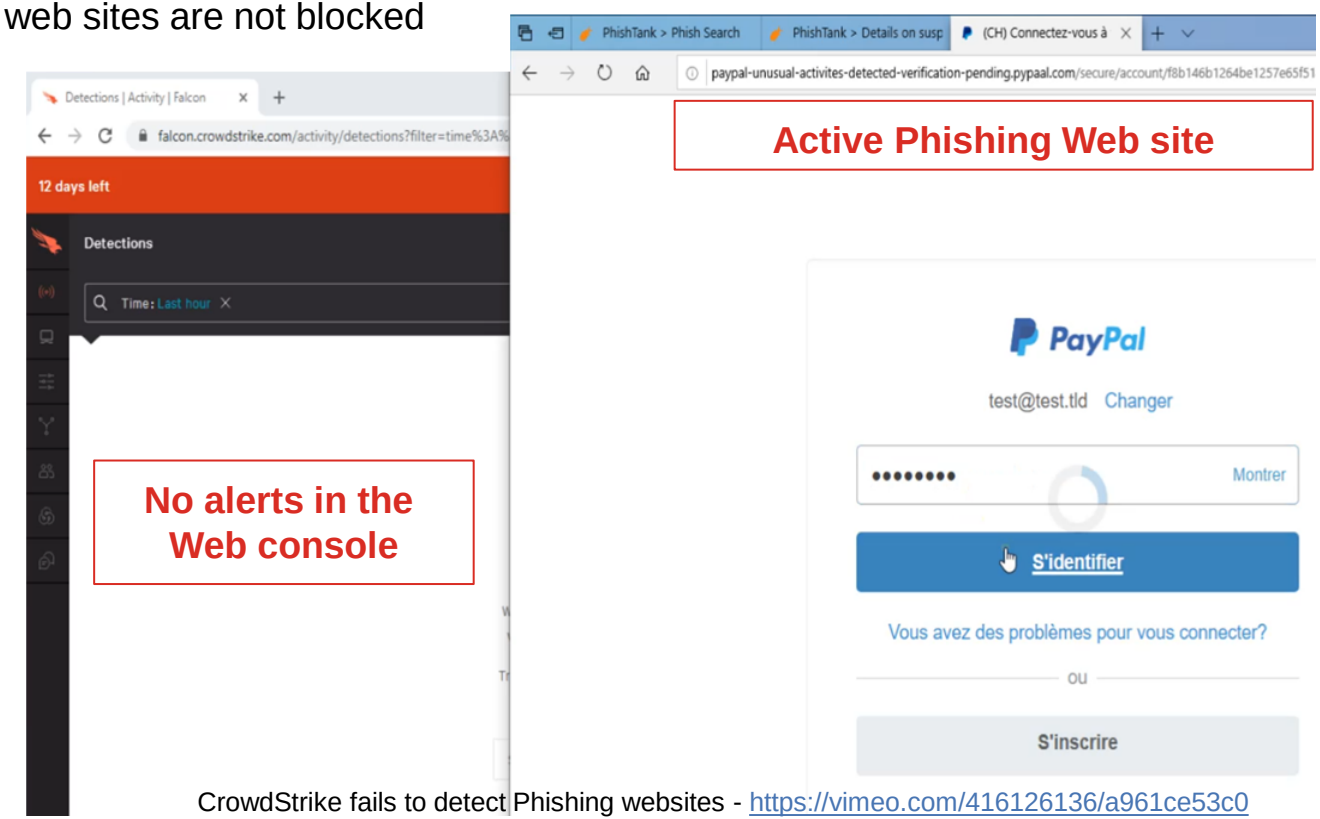
Critical files and registry records of Falcon are not protected



CrowdStrike Anti-Tamper protection bypass - https://vimeo.com/416124290/97858006e3

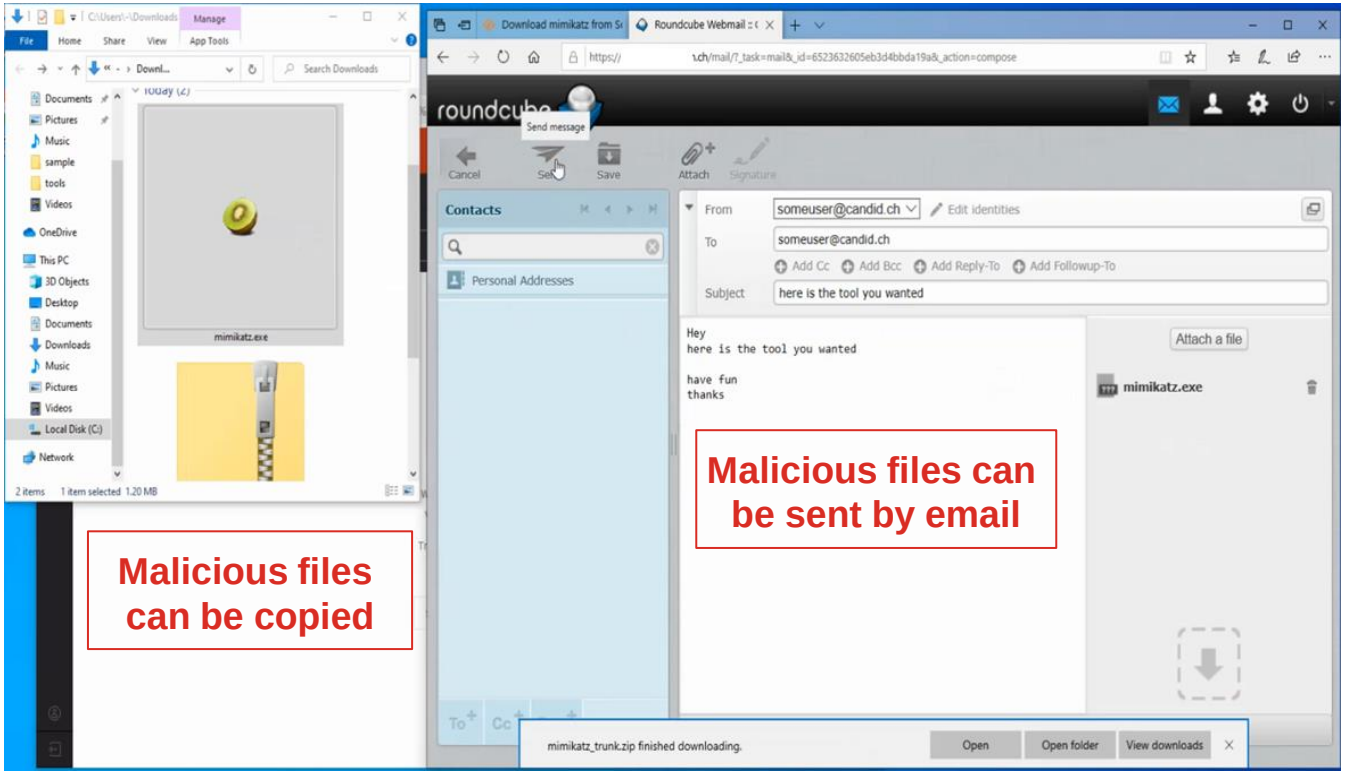
(3) Missing client-side phishing protection

Active phishing web sites are not blocked



CrowdStrike fails to detect Phishing websites - https://vimeo.com/416126136/a961ce53c0

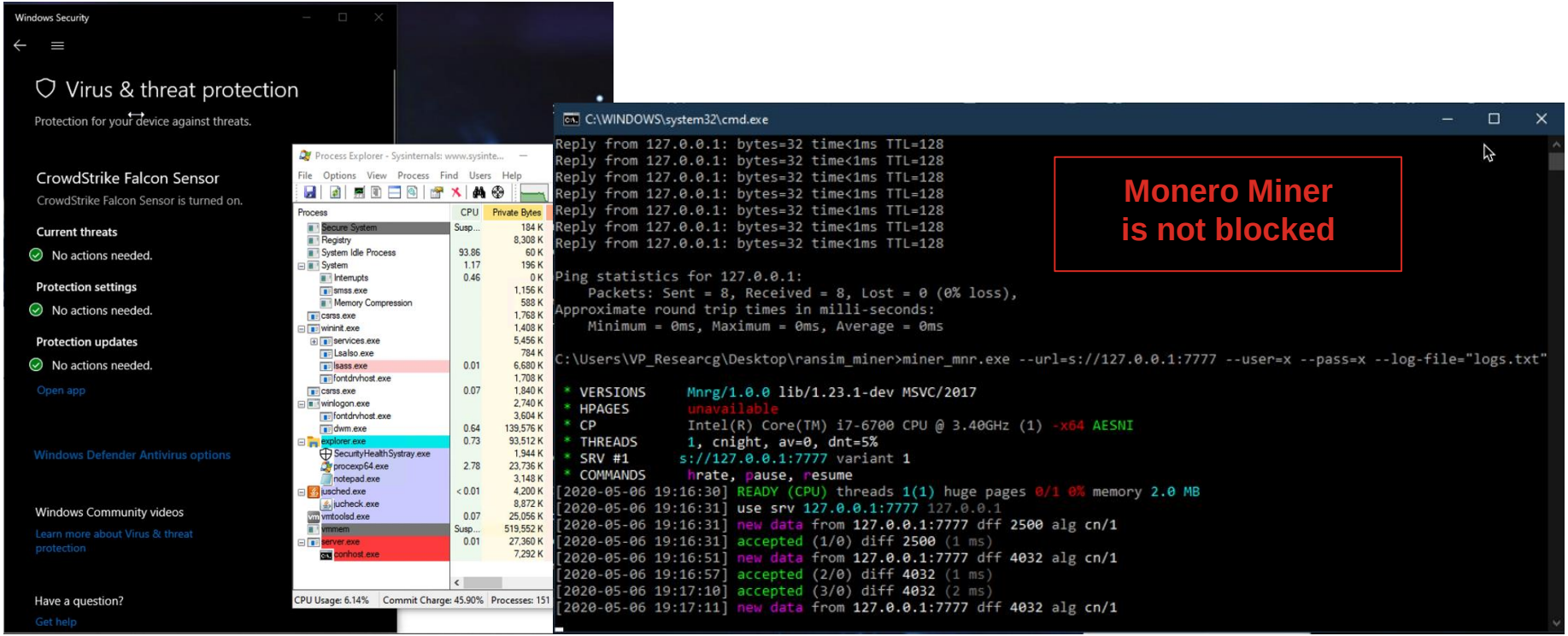
(4) Missing on-access file detection



CrowdStrike fails to block sending of malicious attachment - https://vimeo.com/416126087/c168f09ec0

(5) Missing cryptomining protection

Monero Miner is not blocked by CrowdStrike Falcon



(6) Microsoft Teams and Zoom are not protected

Can allow attackers to steal chats, block users, prevent connectivity

Attacker can remove Teams/Zoom registry keys

Inject code and steal information from chats

Terminate Teams/Zoom to prevent connectivity

- Terminate Process With Remote Thread
- Terminate Process With Remote Thread Dll
- Terminate Process With Section Unmap

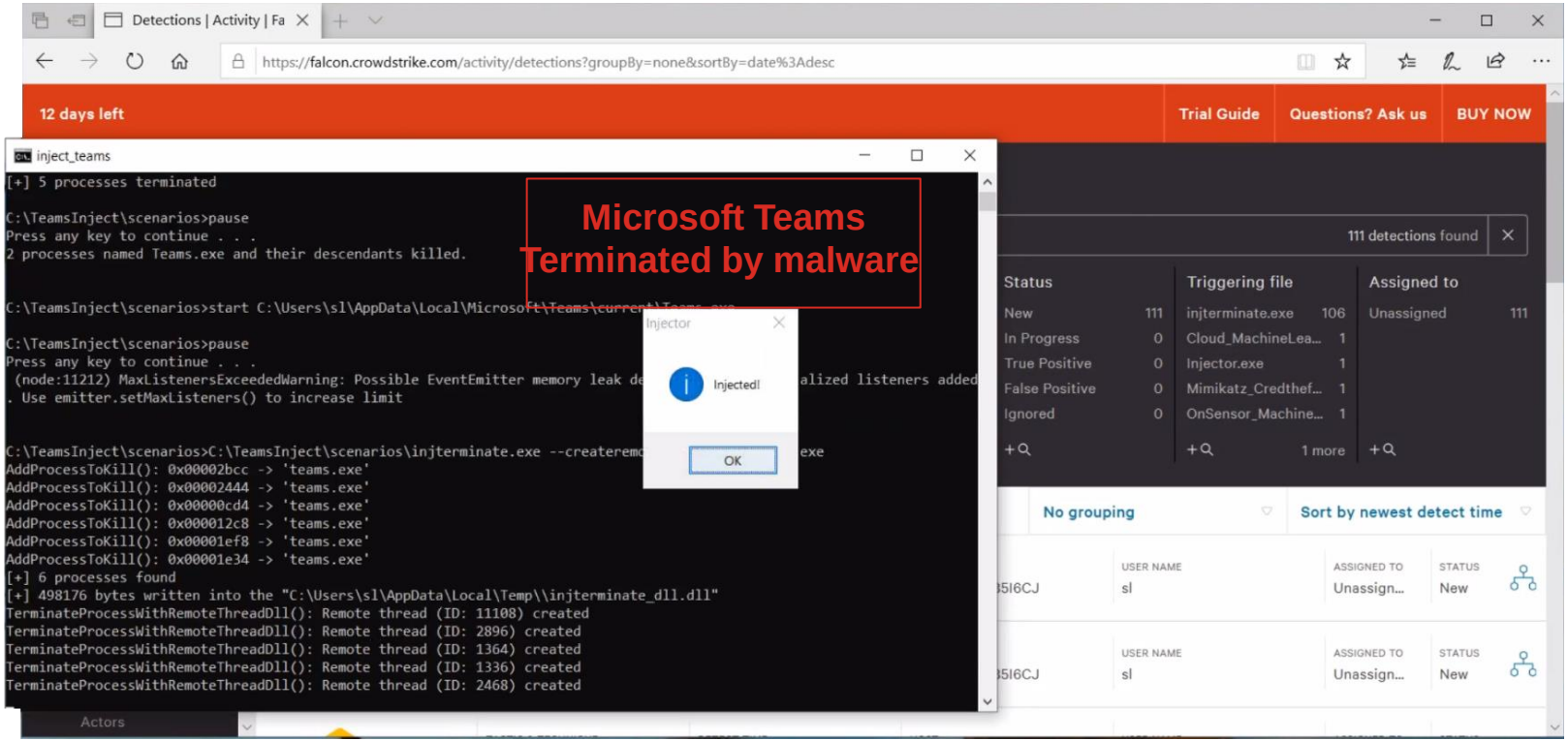
- Teams/Zoom are client side applications and can't protect themself
- DNS attacks based on host file modification is possible
- Latest updates are not forced

Acronis Cyber Protect

- Protection of third-party apps e.g. Microsoft Teams
- Apply the same set of defense techniques

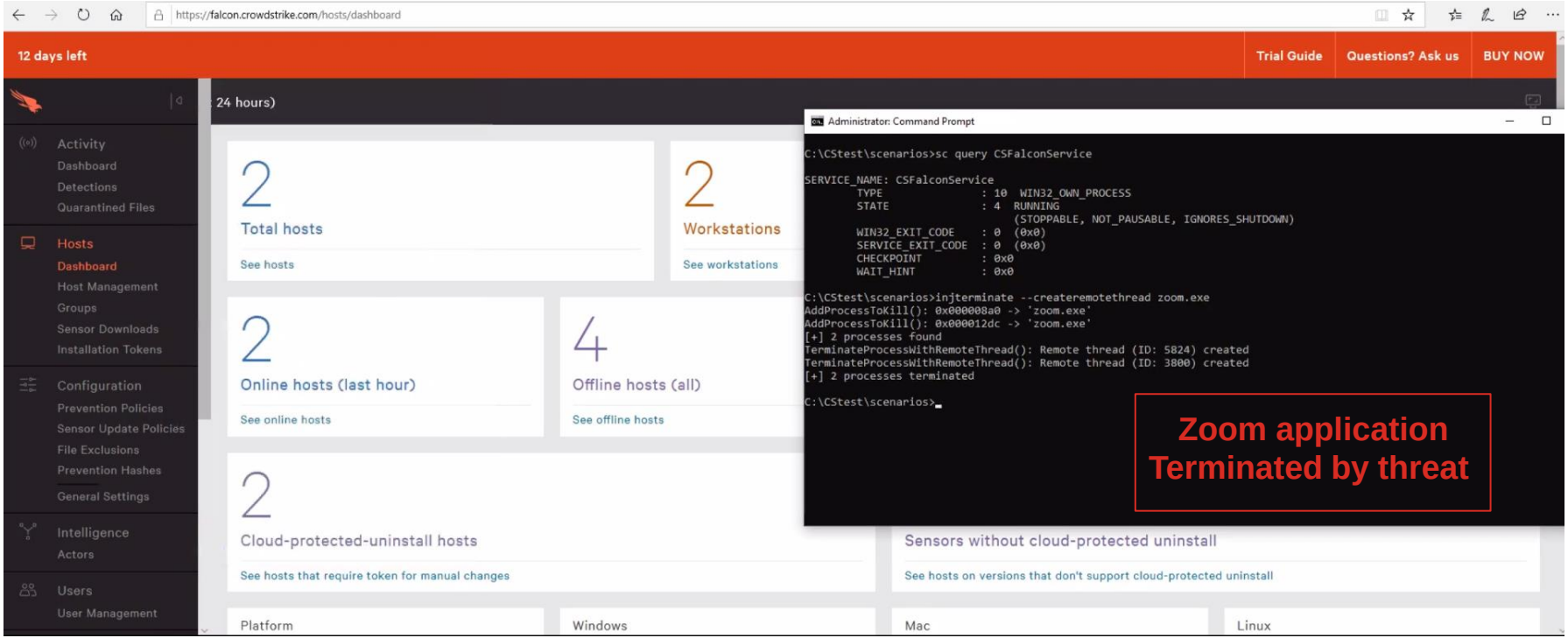
	CS	A
Processes killing		
Processes injections		
Critical files changes		
Critical registry records changes		
Services stop		
Uninstallation protection		

(6) Microsoft Teams is unprotected with CrowdStrike



CrowdStrike fails to protect Microsoft Teams from attacks - https://vimeo.com/416124337/f090df2d17

(6) Zoom is unprotected with CrowdStrike Falcone



CrowdStrike fails to protect Zoom from attacks - https://vimeo.com/416124396/ca305c24fe

Customer case: CrowdStrike Falcon

1. **Weak ransomware protection** → can lead to data loss
2. **Insufficient anti-tamper protection** → can allow attackers to disable the protection
3. Missing client-side **phishing protection** → exposes users to password leaks
4. Missing **on-access file detection** → can lead to malware spreading
5. Missing **cryptomining protection** → can degrade device performance
6. Microsoft **Teams and Zoom** are not protected → can allow attackers to steal chats, etc

CrowdStrike Falcon provides no client-side phishing protection, as well as no email protection; its behavior engine can't protect against advanced ransomware attacks and malicious cryptomining. Anti-tamper protection is limited by processes and services only. Real-time monitoring works only on-execution and won't prevent spreading malicious files via email or shares. No restore capabilities