Highlights

If you live in California, getting homeowner's insurance is becoming a challenge, whether you live in what would traditionally be considered a fire hazard area or in an urban condo. Wildfires took such a toll on the insurance industry that many companies are pulling out of the state entirely. Now, translate that to cybersecurity and ransomware. How do insurance companies assess the risk of a cyber breach, the costs of ransomware, the fact that criminals are targeting companies with the most comprehensive insurance coverage, and increasingly sophisticated cyber attacks? While cyber-insurance companies can look at measures such as attack surface monitoring/intelligence and third-party risk that assess technical vulnerability, the inability to quantify the human part of the equation (employee vulnerability to phishing or other types of attacks, human error, insider threats, etc.) means that a big part of an organization's risk goes unmeasured. This newsletter looks at some of these challenges and the latest cybercrime tactics.

Cheers! Mike Heumann

4 New Thugs in the Ransomware Market

Cybersecurity experts from Palo Alto Networks Unit 42 threat intelligence team have identified four emerging big players in the ransomware criminal industry – AvosLocker, Hive, Linux version of HellyKitty, and LockBit 2.01.

AvosLocker – ransomware as a service, marketing its services via press release branded with a blue beetle logo. They also run a data leak and extortion site and have made ransomware demands ranging from $50-75K. AvosLocker boasts “fail-proof” malware that infects Windows. This ransomware encrypts all user’s data on the PC (photos, documents, excel tables, music, videos, etc), adds its “avos” extension to every file, and creates a GET_YOUR_FILES_BACK.txt file in every folder which contains encrypted files.

Hive – uses spear-phishing emails with attachments. Upon obtaining the user’s network credentials, Hive attempts to infect the network laterally, by using the Remote Desktop Protocol (RDP), targets processes related to backups, anti-virus/anti-spyware, and file copying and terminates them to facilitate

file encryption. The encrypted files commonly end with a .hive extension. The Hive ransomware drops a hive.bat script into the directory, which enforces an execution timeout delay of one second in order to perform cleanup after the encryption is finished by deleting the Hive executable and the hive.bat script. A second file, shadow.bat, is dropped into the directory to delete shadow copies, including disc backup copies or snapshots, without notifying the victim and then deletes the shadow.bat file. During the encryption process, encrypted files are renamed with the double final extension of *.key.hive or *.key.*. The ransom note, “HOW_TO_DECRYPT.txt” is dropped into each affected directory and states the *key.* file cannot be modified, renamed, or deleted, otherwise the encrypted files cannot be recovered. The note contains a “sales department” link, accessible through a TOR browser, enabling victims to contact the actors through a live chat.

Linux variant of HelloKitty ransomware – singles out Linux servers running VMware’s ESXi hypervisor. They have demanded as much as $10M but have captured around $1.48M in actual payments. VMware ESXi, formerly known as ESX, is a bare-metal hypervisor that installs easily onto servers and partitions them into multiple VMs. While that makes it easy for multiple VMs to share the same hard-drive storage, it sets systems up for attacks, since attackers can encrypt the centralized virtual hard drives used to store data from across VMs.

LockBit 2.0 – This ransomware group claims to be the fastest encryption software in the world.

They have compromised 52 organizations in a variety of industries and countries.

The last step of the malware’s infection routine is to change the wallpaper on victim machines to attempt to recruit employees, including information on how organization insiders can be part of the “affiliate recruitment,” with guaranteed payouts of millions of dollars and anonymity in exchange for credentials and network access.

Encryption speed comparative table for some ransomware

PC for testing: Windows Server 2016 x64 \ 8 core Xeon E5-2680@2.40GHz \ 16 GB RAM \ SSD

Name of the ransomware	Date of a sample	Speed in megabytes per second	Time spent for encryption of 100 GB	Time spent for encryption of 10 TB	Self spread	Size sample in KB	The number of the encrypted files (All file in a system 257472)
LOCKBIT 2.0	5 Jun, 2021	373 MB/s	4M 28S	7H 26M 40S	Yes	855	109964
LOCKBIT	14 Feb, 2021	266 MB/s	6M 16S	10H 26M 40S	Yes	146	110029
Cuba	8 Mar, 2020	185 MB/s	9M	15H	No	1130	110468
Babuk	20 Apr, 2021	166 MB/s	10M	16H 40M	Yes	79	109969
Sodinokibi	4 Jul, 2019	151 MB/s	11M	18H 20M	No	253	95490
Ragnar	11 Feb, 2020	151 MB/s	11M	18H 20M	No	40	110651
NetWalker	19 Oct, 2020	151 MB/s	11M	18H 20M	No	902	109892
MAKOP	27 Oct, 2020	138 MB/s	12M	20H	No	115	111002
RansomEXX	14 Dec,2020	138 MB/s	12M	20H	No	156	109700
Pysa	8 Apr, 2021	128 MB/s	13M	21H 40M	No	500	108430
Avaddon	9 Jun, 2020	119 MB/s	14M	23H 20M	No	1054	109952
Thanos	23 Mar, 2021	119 MB/s	14M	23H 20M	No	91	81081
Ranzy	20 Dec, 2020	111 MB/s	15M	1D 1H	No	138	109918
PwndLocker	4 Mar, 2020	104 MB/s	16M	1D 2H 40M	No	17	109842
Sekhmet	30 Mar, 2020	104 MB/s	16M	1D 2H 40M	No	364	random extension
Sun Crypt	26 Jan, 2021	104MB/s	16M	1D 2H 40M	No	1422	random extension
REvil	8 Apr, 2021	98 MB/s	17M	1D 4H 20M	No	121	109789
Conti	22 Dec, 2020	98 MB/s	17M	1D 4H 20M	Yes	186	110220
Ryuk	21 Mar, 2021	92 MB/s	18M	1D 6H	Yes	274	110784
Zeppelin	8 Mar, 2021	92 MB/s	18M	1D 6H	No	813	109963
DarkSide	1 May, 2021	83 MB/s	20M	1D 9H 20M	No	30	100549
DarkSide	16 Jan, 2021	79 MB/s	21M	1D 11H	No	59	100171
Nephilim	31 Aug, 2020	75 MB/s	22M	1D 12H 40M	No	3061	110404
DearCry	13 Mar, 2021	64 MB/s	26M	1D 19H 20M	No	1292	104547
MountLocker	20 Nov, 2020	64 MB/s	26M	1D 19H 20M	Yes	200	110367
Nemty	3 Mar, 2021	57 MB/s	29M	2D 0H 20M	No	124	110012
MedusaLocker	24 Apr, 2020	53 MB/s	31M	2D 3H 40M	Yes	661	109615
Phoenix	29 Mar, 2021	52 MB/s	32M	2D 5H 20M	No	1930	110026
Hades	29 Mar, 2021	47 MB/s	35M	2D 10H 20M	No	1909	110026
DarkSide	18 Dec, 2020	45 MB/s	37M	2D 13H 40M	No	17	114741
Babuk	4 Jan, 2021	45 MB/s	37M	2D 13H 40M	Yes	31	110760
REvil	7 Apr, 2021	37 MB/s	45M	3D 3H	No	121	109790
BlackKingdom	23 Mar, 2021	32 MB/s	52M	3D 14H 40M	No	12460	random extension

Russian Ransomware "Cartel"

Several Russian ransomware cybercriminal gangs have teamed up to share hacking techniques, malware code, infrastructure, and data-breach information. Jon DiMaggio, Chief Security Strategist at Analyst I, provides a comprehensive analysis in Ransom Mafia. Analysis of the World's First Ransomware Cartel. Ransomware code is relatively easy to customize. "A large market of vulnerable computers combined with the pseudo anonymity of cryptocurrency has created an environment ripe for criminal exploitation," explains DiMaggio.

Four gangs exist within the Cartel – Wizard Spider, Twisted Spider, Viking Spider, and LockBit. They are said to exert influence over other smaller ransomware groups and license their tools. The approach of sharing resources, particularly as part of ransomware as a service, allows cybercriminals to pay for the advanced skills of other hackers, with groups such as REvil and DarkSide, providing direct IT support to subscribers. Viking Spider and LockBit upload stolen information to a data breach site hosted and controlled by Twisted Spider. This information is used for phishing attacks that deliver ransomware and posted to criminal name-and-shame sites that are used to embarrass and coerce victims. Twisted Spider also operates a command-and-control server that hosts malware and hacking tools used by other gangs including Viking Spider and LockBit.

There is no indication of actual revenue sharing, so, technically, they are not a cartel. Their cooperation, sharing resources, and reinvestment of profits to bolster their cybercrime objectives do pose a collective threat.

"Analyst1 believes ransomware gangs will focus development efforts to automate attacks. The new capabilities gangs are introducing into their ransomware demonstrate that automation is essential. Analyst1 believes this trend will continue making ransomware operations more efficient and dangerous. As automation capabilities increase, the use of affiliate hackers will decrease. This means ransomware gangs do not have to share profits with affiliates, thus increasing the revenue derived from each attack. With the decrease in the timeframe it takes to execute each attack, Analyst1 believes the overall volume of attacks will grow, raising the number of victims extorted."

Jon DiMaggio

Chief Security Strategist
Analyst I

Can You Prevent Cyber Crime? Insurance Price Hikes Indicate Otherwise.

Cyber insurance premiums are going way up, and Evan Greenberg, Chubb CEO, warns that those increases do not capture the actual risk of a catastrophic cyber event. Prior to the prevalence of ransomware attacks, insurance companies focused on privacy, such as keeping and storing records, versus business interruption costs. Ransomware has radically altered the landscape of cyber insurance and now accounts for 75% of cyber insurance claims. The increase in claims far exceeds the bump in insurance costs. And, there is not a clear path to reducing the risks and capturing the true costs of a breach.

Is paying ransom to criminals driving up insurance costs as the insurance companies themselves feed the cybercriminal enterprise? Companies may focus less on cybercrime prevention knowing that demands will be met; hackers see companies with solid insurance coverage as highly desirable targets for easy payouts.

Deterrence may mean taking a strong stand and not caving to ransomware demands. Anja Shortland, Professor of Political Economy, King's College in London, has extensively studied kidnapping for ransom insurance and says "disruptive bargaining" drove down kidnapper payout demands. In her book, Kidnap: Inside the Ransom Business, Shortland explores the questions of "What exactly is the role of insurers in this system? Would people be safer if insurance did not exist? I see a system that puts the welfare of the hostage centre stage – but also prevents ransom payments from escalating, so as not to put others at risk. Kidnap insurance and the services associated with it thereby facilitate international trade and investment, resource extraction, aid, development initiatives, research and reporting from some of the most complex and hostile security environments in the world. Is this not in the public interest?"

"They've got very clear control of the ransom negotiations, and they tell their customers, "This is how you're going to run this. And, you're not going to panic, Yes, you will get some really horrible threats, and they may say they will take an ear off and they always get that on the fifth phone call. We've yet to receive an ear, so don't cave in." Anja Shortland, discussing how the insurance industry effectively handles kidnap for ransom cases.

Julian Radcliffe, Founding Director of Control Risks, recognizes the application of Shortland's analysis of kidnap ransom insurance claims to ransomware cyber insurance claims, finding her "rigorous analysis is needed not just in this field but also in cyber, art crime and all those areas where the lack of international policing leaves the private sector to find its own solutions…"

Does Crime Pay?

Amateur Attack Group Offers $1M to Entice Employees

Cybercriminals try to trick employees into clinking links to infiltrate and exploit system weaknesses via phishing emails. Additionally, a new approach by a Nigerian criminal enterprise takes a more direct approach. If they cannot trick employees into clicking on links in phishing email, perhaps they can be upfront, and invite them to orchestrate the breach. This group is offering employees a cut of the ransom, initially offering as much as $1M, if employees help sabotage their employer by installing DemonWare on their network. They identify prospective employee targets using LinkedIn.

Researchers at Abnormal Security posed as prospective willing accomplice employees. The criminal group promised the prospective accomplices they would not be caught by their employer because the ransomware would encrypt everything on the system. They instructed them to launch the ransomware physically or remotely and provide two links for an executable file that could be downloaded on WeTransfer or Mega.nz. The criminal group also provided an Outlook email account and Telegram username for the employee to contact them as needed. The researchers determined, “Based on the actor’s responses, it seems clear that he 1) expects an employee to have physical access to a server, and 2) he’s not very familiar with digital forensics or incident response investigations.”

The criminal group claims to have coded the ransomware themselves but DemonWare is freely available from GitHub, placed there by its original author to demonstrate how easy ransomware is to make and use, and is considered one of the least sophisticated forms of ransomware. DemonWare has been around for a few years and was tied to the groups that attacked Microsoft Exchange’s ProxyLogon set of vulnerabilities, CV#-2021-27065, discovered in March.

There are five fundamental types of insider threats:

1. Non-responders to awareness training;
2. Inadvertent insiders;
3. Insider collusion such as with vendor partners;
4. Persistent malicious insiders; and
5. Disgruntled employees.

And, now add 6. Accomplice employees – cash strapped employees and/or employees looking for a quick buck.

Tech Giants Pledge $30B+ Cybersecurity Investment

Tech giants, Amazon, Google, Microsoft, IBM, and Apple have pledged major investments to bolster private and public cybersecurity infrastructure following a meeting with President Biden. The Biden Administration established voluntary cybersecurity goals and is pushing G7 countries to update NATO cyber policy and to aid in a collective effort to hold nations accountable for harboring ransomware criminals.

Amazon – Will provide its internal employee security awareness training directly to individuals and businesses at no charge. They will offer a multi-factor authentication device to AWS account holders to protect against phishing and password theft and the ability to use that device to access applications such as Gmail, Dropbox, and GitHub.

Google – Investment of $10B over the next five years to expand zero-trust programs, help secure the software supply chain, and enhance open-source security. Google will train 100k Americans for data analytics, privacy, and security jobs through its Google Career Certificate program. Additionally, Google intentionally seeks to close both the skills gap and lack of diversity in the industry by targeting unrepresented groups. Half its certificate program graduates are Black, Latinx, female, and/or veterans.

Microsoft – Will spend $20B over the next five years to advance its own security products and services and pledged $150M to improve government agency security posture and expand cybersecurity training partnerships with community colleges and nonprofits.

IBM – Committed to training 150k people in cybersecurity skills over the next three years and partnering with more than twenty historically Black Colleges and Universities to establish cybersecurity leadership centers, to encourage a more diverse cyber workforce.

Apple – Will establish a new program to drive continuous security improvements throughout the technology supply chain, working with its 9,000 US suppliers to drive mass adoption of multi-factor authentication, security training, vulnerability remediation, event logging, and incident response.

AI, Self-Driving Cars, and Advanced Storage

with sponsors NVIDIA, Weka, and b-plus

Is your organization more concerned about storage for data acquisition, training, or operation of AVs? (check one):

Our primary concern is on-vehicle storage for data acquisition:	13%
Our primary concern is on-vehicle storage for data during AV operation:	7%
Our primary concern is on-vehicle storage for both data acquisition and AV operation:	30%
Our primary concern is storage in the lab/datacenter for AI/ML training:	23%
We are not concerned/no opinion:	23%
Other:	3%

When you consider solutions for AI training and data acquisition, what factor is most important to your organization? (check one):

Cost:	23%
Storage capacity:	13%
Storage performance:	45%
Storage networking:	10%
Future expandability:	3%
Other issues:	6%

G2M Research Multi-Vendor Webinar Series

Our webinar, Tuesday, August 17, "AI/ML Storage – Distributed vs Centralized Architectures", sponsored by Weka, AIC, and Excelero, is available. View the recording here and/or download a PDF of the slides. Register for our webinars and we will send these recordings directly to you.

Our webinar schedule is below- Click on any of the topics to get more information about that specific webinar. Interested in sponsoring a webinar? Contact G2M for a prospectus. You can view all our webinars and access all the slide deck presentations.

We also host custom webinars and webinar series as another highly effective approach to reach your target audience – before the webinar(s) with direct and social media marketing, during the webinar with a customized presentation and audience polls, and after the webinar with use of the recording and presentation materials for outreach. Join us for our KIOXIA series.

Oct 12: Cloud Service Providers: Is Public Cloud, Private Datacenter, or a Hybrid Model Right for You?

Many cloud service providers start their business utilizing "public cloud" compute and storage resources to run their applications, but look to build their own datacenter as their business grows and the cloud becomes expensive.

This webinar looks the key factors driving the decision between public cloud, a private datacenter, or a hybrid approach for cloud service providers.

Nov 9: The Radiometry Data Explosion: Can Storage Keep Pace?

At the intersection of artificial intelligence, petabyte-scale storage, and cutting-edge computing is radiometry, the study of millions of medical images to speed up the time to diagnosis of cancers.

This webinar explores the various storage architectures and data management tools necessary to keep up with the growth in high-resolution imagery for radiometry.

Dec 14: 2021 Enterprise Storage Wrap-up Panel Discussion

Join G2M Research and a panel of industry experts to discuss the major enterprise storage tends, innovations, events and happenings of 2021, and what to expect as we head into 2022.

AI & Cybersecurity Events

September 14-15	Virtual Cybersecurity & Fraud Summit: London
September 15-16	ODSC APAC
September 16	Miami/South Florida Virtual Cyber Security Summit
September 16	Interface Sacramento Reno
September 16-17	Cyber Security Summit & Hacker Conference
September 16-18	Global Artificial Intelligence Conference
September 20-22	Gartner Security & Risk Management Summit
September 21	HackerOne Security
September 22-23	The AI Summit London 2021
September 22-24	Cyber Senate Control Systems Cybersecurity USA
September 23	SecureWorld Great Lakes Virtual Conference
September 27-29	GSX 2021
September 28-29	International Cyber Expo London
September 29	European Legal Security Forum 2021
September 29-30	AI & Big Data Expo – North America
October 4-8	Cyber Defense Summit 2021
October 8-9	THOTCON 2021
October 14	SecureWorldExpo
October 19-20	IAPP Privacy. Security. Risk. 2021
October 20-21	Counter-Insider Threat Symposium
October 20-21	DevSecCon London
October 25-27	InfoSec World 2021

G2M RESEARCH

Effective Marketing & Communications
with Quantifiable Results