Security Now! #721 - 07-02-19

Exposed Cloud Databases

This week on Security Now!

This week we track further occurrences of Ransomware in Florida and elsewhere, we check-in on the state of the "Going Dark" anti-encryption debate, we look at a new stunning BlueKeep Proof of Concept demo produced by the guys at SophosLabs, we update some miscellany and closing the loop feedback from our terrific listeners, then we examine the nature of the continuing problem of massive publicly-exposed databases. In the third example of this just this week, we discover a prolific Chinese IoT manufacturer who is logging more than a million of their customer's devices into a massive 2+ billion record publicly-exposed database, which returns us to the dilemma we have with the utter lack of oversight and control over our own IoT devices, and the need to soberly rename what IoT is an abbreviation for.

And our picture of the week is quite apropos:

Security News

More ransomware news from Florida...

On June 10, the computers of the Lake City, Florida (population 12,000) ceased to function as malware encrypted their data after they were hit by a powerful ransomware attack named "Triple Threat" because it mixes three different methods of compromise. An employee opened a document they received via email, which infected the city's network with the Emotet trojan, which later downloaded the TrickBot trojan, and later, the Ryuk ransomware.

Although the affected system were disconnected within minutes of the discovery that something was very wrong, the malware was still able to infect systems controlling most of the city's land-line phones and email systems, forcing employees to use pen and paper in an attempt to continue working. Fortunately, police and fire and other emergency services remained unaffected because they were on a separate network.

A week after the attack a request for ransom was received from the attacker. This request was sent to the Florida League of Cities, the insurance provider for the City of Lake City. The League began negotiating with the attacker and agreed to pay 42 bitcoins ($400,085.00). I was interested to hear that the attackers sent the ransom demand to the city's insurance carrier. That suggests a bit more sophistication than I'd have expected.

The City's Information Technology Director Brian Hawkins said: "Our systems are shut down, but there is no evidence to indicate any sensitive data has been compromised. All customer service payment data, such as credit card data, is stored off-site by third-party vendors and would not have been accessed by an attack like this on our network."

However... (Whoops!...) With no proper backup to restore the data, Lake City was left with no option but to pay the ransom. Thus, the city's leadership approved the ransom payment last Monday, 42 Bitcoins were paid last Tuesday, and the city's I.T. staff began decrypting files later the same day.

Mayor Stephen Witt said that the administration made the decision to pay up after talking with the FBI and the city's insurance company. Fortunately for the City, and less so for their insurance company, the Mayor said that most of the money is covered by the insurance except for a $10,000 deductible, which will be supported by the citizens by paying a higher insurance rate in the future. The Mayor also told a local TV news station that a city employee had been fired. But it wasn't the person who clicked on the eMail. The city's I.T director, Brian Hawkins, whom we quoted earlier trying to paint a sunny smile on the situation... was fired.

So... 42 Bitcoins this week and 65 the week before from the Florida city of Riviera Beach. That's 107 Bitcoin currently valued at: $1,360,000.

And so this creates a dilemma. Attackers have apparently found an interesting niche to attack: Like individuals, smaller government municipalities lack sufficient I.T. infrastructure to allow them to both protect from and recover from targeted attacks. But unlike individuals, they have MUCH more important data at stake, as well as insurance to take the short term sting out of paying.

Okay, so everyone who is listening to this podcast, raise your hands of you think that the bad guys have all the money they want and will stop pestering deep-pocketed (or at least well-insured) small municipalities with targeted attacks. Anyone? No? That's right. We're going to be seeing more of this.

OH! And guess what!! That's already happened! Since then, an even smaller village of just 3,000 residents, the Florida municipality of Key Biscayne was hit. Officials reported a Ryuk ransomware infection last week, but they haven't decided yet if they want to pay the ransom demand. A special session of the Village Council of Key Biscayne was held last Friday night, with a second session on Saturday, to determine how to respond to the Ryuk ransomware attack on the village's systems. Local officials have not responded yet to questions on the outcome of that meeting.

Recently, the public and media have turned negative on city officials who fail to secure networks and then decide to pay hackers. Paying ransom demands is now viewed as a sign of a city administration's failure and weakness, rather than a quick fix to get access back to citizens' data.

And as we would expect, in all of these cases, forensics determined that a city employee ushered the malware into the network by opening a malicious email. So whatever backup policies and systems may have been in place -- if any -- apparently did not function properly.

Oh, and just as I was trying to wrap up this story... The state of Georgia's Judicial Council and Administrative Office of the Courts fell victim to a Ryuk ransomware attack.

Meanwhile, the "Going Dark" problem is NOT going away. (And it's not going to.)
A headline in Forbes caught my eye:
"U.S. May Outlaw Messaging Encryption Used By WhatsApp, iMessage And Others"
https://www.forbes.com/sites/zakdoffman/2019/06/29/u-s-may-outlaw-uncrackable-end-to-end-encrypted-messaging-report-claims

I thought "WHAT?!?!... how did I miss that?!?!" And, of course, the headline was more speculation that anything. But, strictly speaking, it's true that the U.S. may do something, and likely will. So I tracking down the article's source, which turned out to be a piece in Politico titled: "Trump officials weigh encryption crackdown"
https://www.politico.com/story/2019/06/27/trump-officials-weigh-encryption-crackdown-1385306

I've trimmed it way down to remove most of the superfluous fluff and stuff we all know, but there are some interesting bits left, and it's useful for getting a sense for the environment:

Senior Trump administration officials met last Wednesday to discuss whether to seek legislation prohibiting tech companies from using forms of encryption that law enforcement can't break.

The encryption challenge, which the government calls "going dark," was the focus of a National Security Council meeting Wednesday morning that included the No. 2 officials from several key agencies, according to three people familiar with the matter.

Senior officials debated whether to ask Congress to effectively outlaw end-to-end encryption.

One of the people interviewed said: "The two paths were to either put out a statement, a general position on encryption and [say] that they would continue to work on a solution... or to ask Congress for legislation."

But the unreported meeting of the NSC's so-called Deputies Committee did not produce any decision.

A decision to press for legislation would have far-reaching consequences for the privacy and security... effectively forcing companies such as Apple and Google to water down the security features on their smartphones and other devices.

A ban on end-to-end-encryption would make it easier for law enforcement and intelligence agents to access suspects' data. But such a measure would also make it easier for hackers and spies to steal Americans' private data, by creating loopholes in encryption that are designed for the government but accessible to anyone who reverse-engineers them. Watering down encryption would also endanger people who rely on scrambled communications to hide from stalkers and abusive ex-spouses.

POLITICO was unable to determine what participating agency leaders said during the meeting, but there is a well-known fault line on encryption within the executive branch.

The DOJ and the FBI argue that catching criminals and terrorists should be the top priority, even if watered-down encryption creates hacking risks. The Commerce and State Departments disagree, pointing to the economic, security and diplomatic consequences of mandating encryption "backdoors."

DHS is internally divided. The Cybersecurity and Infrastructure Security Agency knows the importance of encrypting sensitive data, especially in critical infrastructure operations, but ICE and the Secret Service regularly run into encryption roadblocks during their investigations.

An NSC spokesperson declined to comment on the meeting.

The high-level NSC discussion highlights how policymakers have continued grappling with encryption even as it has receded from the headlines.

"There is a significant [administration-]wide effort underway on what to do about the going dark issue," said a lobbyist familiar with the discussions.

Tech companies such as Apple and Google began increasing their use of end-to-end encryption in 2014, to address privacy concerns sparked by former NSA contractor Edward Snowden's disclosures about the vast sweep of U.S. government surveillance. In response, DOJ and the FBI reinvigorated a decades-old campaign against this feature, arguing that it posed an impenetrable roadblock in many criminal and counterintelligence investigations.

The 2015 San Bernardino, Calif., terrorist attack brought the encryption debate into the mainstream when DOJ took Apple to court to access a locked iPhone belonging to one of the shooters. Then-FBI Director James Comey accused Apple of trying to create a space beyond the reach of U.S. law. But that dispute ended without a definitive legal precedent, and despite the "going dark" problem occasionally resurfacing, encryption hasn't made major headlines for years.

The transition between the Obama and Trump administrations saw a hand-off of sorts between two high-profile advocates of the need to access encrypted data. After President Donald Trump fired Comey, Deputy Attorney General Rod Rosenstein succeeded him as the government's top "going dark" warrior. Rosenstein, who dealt with the issue as a U.S. attorney, warned vaguely that cooperation with Silicon Valley was unlikely to work, implying that legislation might be needed.

But now Rosenstein is gone, and experts generally agree that Congress is unlikely to pass a bill requiring warrant-compatible encryption.

[Interesting term. This is the first time I've seen the term: "warrant-compatible encryption."]

Sens. Richard Burr (R-N.C.) and Dianne Feinstein (D-Calif.) floated a draft measure in 2016 after the San Bernardino attack, but an intense backlash quickly killed its prospects, and despite occasional rumblings, it has not reappeared since. The climate is no better for the administration in the Democratic-controlled House, where there is bipartisan opposition to undermining encryption.

Still, the decision to hold an NSC deputies meeting — which has happened rarely under national security adviser John Bolton — suggests that the issue may not remain on the back burner for long.

=====
So the presumption is that this sort of sentiment-gauging meeting might be preliminary to more public and open talks.

In any event, as I followed links from this story, I discovered the Lawfare Blog, and its back and forth discussions about a proposal by the UK's GCHQ for what is being called, I kid you not, "The Ghost Protocol." It's interesting, and we don't have time this week to dig into it, but I think that it will likely be next week's topic... since it represents the first serious attempt at a firm government-sourced compromise beyond the current "all or nothing" fight we've had so far. And... the security industry is not at all happy about it.

SophosLabs STUNNING BlueKeep PoC demo video...
Kevin Beaumont / @GossiTheDog
"Sophos have made an incredible #BlueKeep exploit (not public) which changes the Windows accessibility shortcuts, so you can bypass RDP login screen and get a GUI session."
https://vimeo.com/344915265
http://grc.sc/bluekeep

SQRL

Joshua @ovalwonder
I have a question regarding a unique use case of SQRL. I am active duty military, and am frequently using controlled systems that don't allow installation of third party software, including browser extensions. I also work either on underway ships or in areas where cell phones and other electronic devices are prohibited. Is there any way for SQRL to work for me? I tried to sign up for the forum, but my account is in moderation.

GMT @gordonmytuba
Searched for sqrl app on iTunes, found this: sqrl.chat

Miscellany

I Am Mother
"Such an underrated piece of Sci-Fi!" (https://www.imdb.com/review/rw4923158/)

Nguyenbakhanhbicondova 9 June 2019
The reviews I read only gave me the impression that this would be a decent thriller, not...this. After watching one generic blockbuster after another, it's always so nice to see small, creative films like "I Am Mother" are still getting made. I'm really curious about how much this film cost, because it looks really impressive, but I also have the feeling that it has a very small budget. This film has solid acting and interesting characters, it touches on complicated ideas with a tightly paced narrative from start to finish and managed to keep me on the edge of my seat till the very end. If you love to treat yourself to some great science fiction, I highly recommend "I Am Mother."

From a Security Now! listener:
In the most recent Security Now, Steve mentions a link he was going to send to Leo of a review of I Am Mother, written by a guy who created an account on IMDb solely to post about the film. Did he ever share that URL during the podcast or in the show notes? I would love to read that review, but I haven't been able to spot it by idly browsing through all the reviews of that film on IMDB, nor by browsing/searching transcripts or skimming through the episodes.

WARNING!! MEGA-SPOILERS!!

The review is here: https://grc.sc/iam

When the IMDB page opens, the review is closed, since it's long. So click on the little down arrow at the lower right.

GRC.SC

Note that this is the maiden deployment of GRC's link shortener where 'sc' stands for "Short Cut" I've been intending to bring up my own link shortener for the podcast and for other miscellaneous needs. Someone noticed that I had been using bit.ly/SN-### links and jumped ahead to create some mischief. I had GRC.SC for "shortcut" for quite a while but I never pulled the trigger.

SpinRite

Howdy Steve and team,

My name is Bob Johnson. I've been using Spinrite since ver 5. During that time I was in the United States Air Force and was my fighter squadrons SCM (small computer manager). Basically, I was THE I.T. dept. We had a copy of SpinRite v5 (I can not vouch for its license... but we used it to recover **many** a crashed drive!

So, when Spinrite 6 came out in 2004 I immediately bought one for myself. It was the best money I have ever spent, hands down.

So now I'm fervently awaiting ver. 6.1. I have caught you from time to time mentioning your group of testers. I would like to be one of them. Am I correct in my understanding that only those that find their way to your forum/usefeed/hideaway of testers get to beta test? OK then, challenge accepted. When I have time to poke around, I'll find you guys. In the meantime, reserve me a copy of whatever the latest version is!

Take care, see you around.

Bob Johnson, avid Spinrite user, Ketonian, and defeater of diabetes. The later thanks to you and your selfless research with your own n=1 Ketogenic experiment.

Closing The Loop

Alan Turing / @CyberWarrior010

"Steve! Not sure you have heard about this get, so I thought I would drop it in your ear. I have found an Exim worm that is, get this, patching the Exim vulnerability. Fun Stuff. I have screenshots if you're interested."

James Alseth / @allset_

"There are no bugs" that's a hell of a claim, what test suites do you run? What are your testing processes?

Spencer Dailey / @SpencerDailey

Hello again Steve - this is a neat thing about uBlock origin, probably worth mentioning -- I remember back when you were deciding to switch from NoScript to uBlock Origin, and at the time - it was presented as a monolithic "Do I run javascript or not?" dilemma. Since then, uBlock Origin has added the ability to disable javascript on a “per-site” basis (it's the icon that looks like a script in the bottom right of the popup). It would probably be good to let listeners know that they can selectively disable javascript on a site-by-site basis -- for a pretty big security and performance gain! cheers, and a shout out would be cool! Spencer Dailey from Austin

Exposed Cloud Databases

I've commented recently that I often don't bother to mention the more or less continuous flow of reports of publicly and inadvertently exposed "Cloud-based" databases. They're not super-interesting and there's no real take-away from each episode. If we had access to the internal details of each breach, so that we could see exactly how each one happened THAT would make for some fascinating and probably teachable moments.

But every one of these breaches must come down to two pivotal mistakes:

First, probably without exception, the data was never intended to be made public. So the database should never have been "bound" to the public-facing server interface. So, the developers of these database systems wrongly assume that network-savvy engineers will be setting up these systems and will know better.

Second, also without exception, ALL access to the data, even internally, should be protected by some form of strong authentication mechanism, preferably several.

Only if BOTH of those "absolutely must do" measures have been ignored can we have problems such as are occurring constantly out on the public Internet. And it's not accurate to call these "data breaches", though the tech press often does, I guess because that sounds sexier. It's not a data breach when a web browser is used to access a website because a web server is publishing the website's contents. So neither is it a "data breach" when a database has been PUBLISHED by a database server onto the public Internet so that anyone who queries the server will obtain the database's data. It might have been an inadvertent publication of that data, but no "breaching" of anything was required to obtain access. It was being openly served and publicly exposed.

So, this week, yet again, several recent data EXPOSURES came to light...

In the first instance, more than 5 million records containing personal information and medical insurance data were exposed in a database belonging to the insurance marketing website MedicareSupplement.com. MedicareSupplement.com is a U.S.-based marketing site which allows visitors to find supplemental medical insurance available in their area. Last Thursday, researchers said that they found this publicly-available MongoDB database that had been online for several days and was unprotected by any password or other authentication.

Bob Diachenko, who discovered the database along with researchers at Comparitech, told Threatpost “While I have not seen any ransom notes or suspicious activity, the IP in question has been first indexed by a public search engine BinaryEdge on May 10. With a MongoDB exposed in the wild for such a long time, there is a very high likelihood that it has been accessed by others.”

Those 5 million records contained personal and personally identifiable data including first and last names, physical addresses, IP addresses, email addresses, dates of birth, and gender. The database also included an array of specific marketing-related information for customers such as lead duration. And within those, approximately of the 239,000 records also indicated the areas

of interest for customers – for instance, medical insurance (i.e. cancer insurance), as well as life, auto, and supplemental insurance.

The researchers disclosed the presence of the vulnerable database to MedicareSupplement.com, after which the database access was disabled and proper security was put in place.

Also in the news this past week were three publicly-accessible cloud storage buckets from an Israel-based data management company "Attunity" which leaked more than a terabyte of data (yes, that's more than 1000 Gigabytes) of data belonging to half of the Fortune 100 enterprises. The leaked data included internal business documents, system passwords, sensitive employee information.

UpGuard, the group who discovered the open data wrote-up their discovery under the title: "Data Warehouse: How a Vendor for Half the Fortune 100 Exposed a Terabyte of Backups"

<quote> The UpGuard Data Breach Research team can now disclose that a set of cloud storage buckets utilized by data management company Attunity have been secured from any future malicious action. Attunity, recently acquired by business intelligence platform Qlik, provides solutions for data integration. An UpGuard researcher discovered three publicly accessible Amazon S3 buckets related to Attunity. Of those, one contained a large collection of internal business documents. The total size is uncertain, but the researcher downloaded a sample of about a terabyte in size, including 750 gigabytes of compressed email backups. Backups of employees' OneDrive accounts were also present and spanned the wide range of information that employees need to perform their jobs: email correspondence, system passwords, sales and marketing contact information, project specifications, and more.

On May 13th, 2019 an UpGuard researcher discovered publicly accessible Amazon S3 buckets named "attunity-it," "attunity-patch" and "attunity-support." The oldest files in "attunity-it," where the bulk of the sensitive data was stored, were uploaded in September of 2014, though that does not necessarily mean they were publicly available at that time. The most recent files had been uploaded just days prior to the researcher discovering the bucket. [So the bucket was in active use at the time of its discovery and contained at least five years of archived customer data.] The researcher notified Attunity on May 16, 2019. As a result of time zone complications, and due to Attunity having been recently acquired by Qlik, the researcher ultimately wound up speaking on the phone with Qlik support. By the next day, public access to the buckets had been removed.

In previous cases, we have discussed the complexity of fully analyzing and describing data stores that contain copies of users' workspaces and mailboxes. Work lives are spread across countless files, each one with some importance, but difficult to reduce to any single metric of significance. While various tools can help search across large data stores, gaining those quantitative measures comes at the expense of analyzing the qualitative nature of the data. There may be a large number of email addresses, for example, but whether they are enterprise customers or merely marketing targets changes the significance of their inclusion. A few key examples from the Attunity data set can illustrate the kinds of data that users have access to and which can be exposed by misconfigured storage of those users' file collections, as in this exposure of Attunity data.

According to Attunity's website, more than two thousand enterprises and half the Fortune 100 use Attunity.

A[nd, sure enough, a] file with a client list found in the repository included a client list with a number of companies commensurate to that description. Every business must have customers, and having commercial relations entails some exchange of information, leading many data exposures to involve third party data for customers or other involved entities. In this case, Attunity's business in cloud migration and data integration also involves supplying and managing the software that processes customer data. Exhaustively documenting the files associated with each of thousands of companies is not feasible or necessary for the research team's purpose of raising awareness of the risk of data leaks. As in past reports, a few examples can highlight the kinds of information that can be exposed through misconfigured storage, and were exposed in the case of Attunity.

[[There description page is horrifying even after being heavily redacted for responsible disclosure. Things like password reset eMails, eMail say: "This is your VPN PIN and password..." And much much more. The idea of all of this data having been publicly exposed for who-knows-how-long is sobering. And depending upon whose hands this fell into, it could have devastating consequences for Attunity's Fortune 100 and several thousand other enterprises. The tech press noted that NetFlix, TD Bank and Ford were among the companies whose data was included in the data exposure.

The conclusion to UpGuard's write-up made a great point:]]

Conclusion

Attunity's business is to replicate and migrate data into data lakes for centralized analytics. The risks to Attunity posed by exposed credentials, information, and communications, then are risks to the security of the data they process. While many of the files are years old, the bucket was still in use at the time detected and reported by UpGuard, with the most recent files having been modified within days of discovery.

The chain of events leading to the exposure of that data provides a useful lesson in the ecology of a data leak scenario. Users' workstations may be secured against attackers breaking in, but other IT processes can copy and expose the same data valued by attackers. When such backups are exposed, they can contain a variety of data from system credentials to personally identifiable information. Data is not safe if misconfigurations and process errors expose that data to the public internet.

=====
The point here is that an attacker needn't try to seduce their way into an enterprise's workstations to look around when their full backups are available for the taking due to the misconfiguration of an affiliated 3rd-party cloud services provider.

Remember, UpGuard wrote: "The total size is uncertain, but the researcher downloaded a **sample** of about a terabyte in size..." Just imagine what bad guys in a hostile nation could do with terabytes of eMail, passwords, internal communications and backups of the top U.S. companies.

..... And we're not done yet, because... also this past week
vpnMentor reports: "Orvibo Smart Home Devices Leak Billions of User Records"

Our expert cybersecurity research team, led by Noam Rotem and Ran Locar, discovered an open database linked to Orvibo Smart Home products. The database includes over 2 billion logs that record everything from usernames, email addresses, and passwords, to precise locations. As long as the database remains open, the amount of data available continues to increase each day.

Orvibo claims to have around a million users. These include private individuals who connected their homes, as well as hotels and other businesses with Orvibo smart home devices. [Amazon sure knows about them!! ... Tons of IoT offerings.]

This constitutes a massive breach of privacy and security with far-reaching implications. The data breach affects users from around the world. We found logs for users in China, Japan, Thailand, the US, the UK, Mexico, France, Australia, and Brazil. We expect that there are more users represented in the 2 billion plus logs.

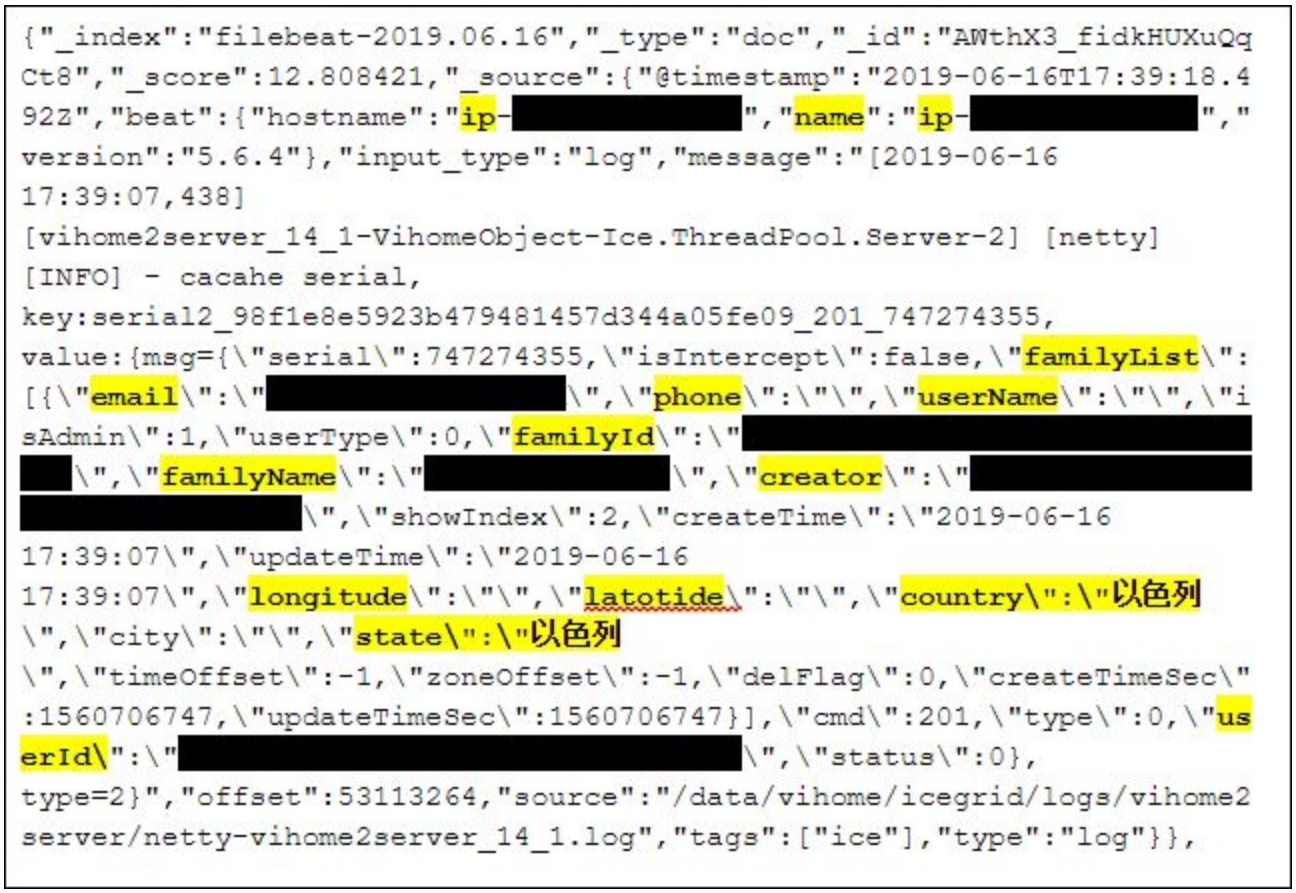
We first contacted Orvibo via email on June 16. When we didn't receive a response after several days, we also tweeted the company to alert them to the breach. They still have not responded, nor has the breach been closed.

The amount of data available from Orvibo's servers is enormous. It's also highly specific, which shows just how much data smart home devices can collect about their users. According to the company, there are over a million users who have installed Orvibo products in their homes and businesses.

The Chinese company, based in Shenzen, manufactures 100 different smart home or smart automation products.

Data Included in the Breach

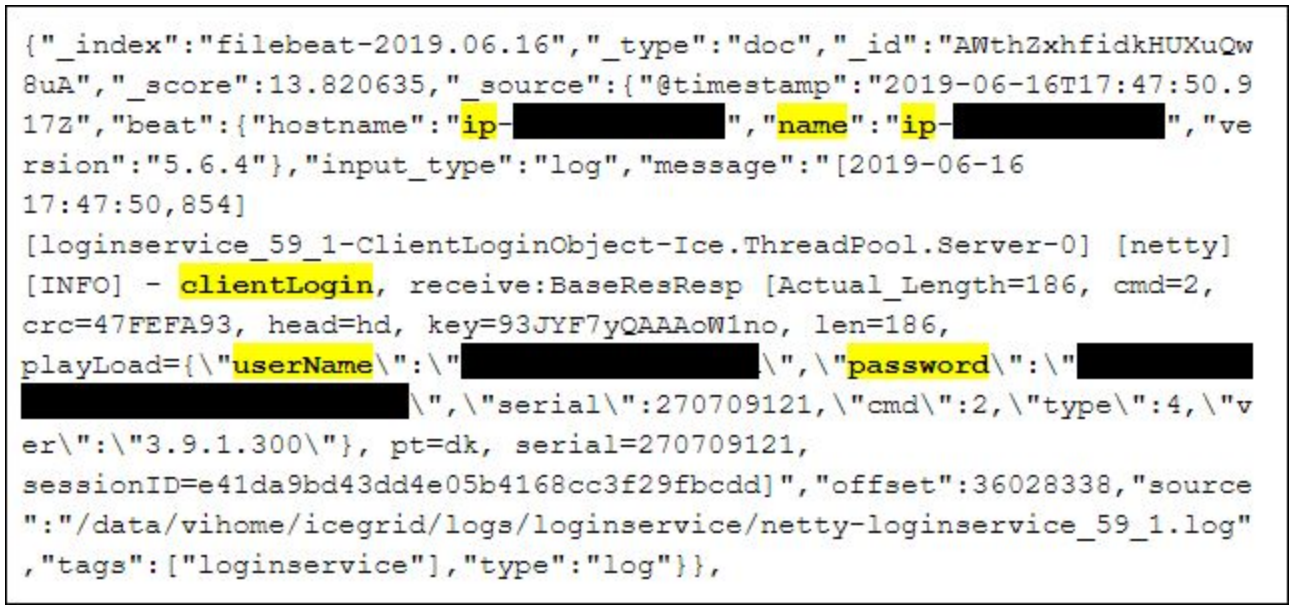
- Email addresses
- Passwords
- Account reset codes
- Precise geolocation
- IP address
- Username
- UserID
- Family name
- Family ID
- Smart device
- Device that accessed account
- Scheduling information



https://www.vpnmentor.com/wp-content/uploads/2019/06/orvibo-1.png

In this first example, we can see that Orvibo is collecting a large amount of data about its users. In this case, not all of the data points are recorded; however, we have other examples that include very specific geo-data, chosen family names, usernames, passwords, and the reset codes that would allow for account takeover.

https://www.vpnmentor.com/wp-content/uploads/2019/06/orvibo-password-2.png



https://www.vpnmentor.com/wp-content/uploads/2019/06/orvibo-password-1.png

These data logs are for the same account, which we can verify with the matching email address and user ID number. In the first, we only have the email address, IP address, and a reset code. With this code accessible in the data, you could easily lock a user out of their account, since you don't need access to their email to reset the password.

The code is available for those who want to reset either their email address or password. This means a bad actor could permanently lock a user out of their account by changing first the password and then the email address. Orvibo does make some effort into concealing the passwords, which are hashed using md5 without salt.

The above example is a small sample of the kind of geolocation data we have. Orvibo keeps logs of precise longitude and latitude coordinates (spelled latotide in the data). The precision of the coordinates can lead us to a user's exact address. This also demonstrates that their products track location in their own right, rather than determining location based on an IP address.

In this entry from a user in Mexico, it shows exactly which device the user was connected to when the data was logged. According to the Orvibo website, HomeMate is a full smart home system that employs a full range of their products to connect your entire home. This amount of data shows just how vulnerable a user can be should a hacker take advantage of this breach.

One of the products Orvibo offers is a smart mirror. This includes technology to show the weather and display a schedule. Here, we have a log for the schedule the user has set with a customized name. "Winter week AM" giving us precise information about the user's calendar.

This is a data log that includes a large number of devices connected to a single account. We can see a clear record of the user having one of Orvibo's smart cameras. Another device is named "massage room." Though not all of the device names tell us which device is where, it could help someone pinpoint a device to hack if they wanted to do so. The "massage room" label also points towards this data likely belonging to a business.

Another Smart Camera log included a message that was recorded word for word. That opens the possibility of a user revealing even more personal information through their account.

It's important to note that not every single data log included every type of personal information. However, even with over 2 billion records to search through, there was enough information to put together several threads and create a full picture of a user's identity.

[[Also stop to consider that this is a Chinese company based in Communist Shenzen China. The concern here is with a massive and incredibly irresponsible disclosure of extremely sensitive customer data. But even if this massive multi-billion record database were not exposed... it is STILL being gathered and retained. But to what end and purpose?]]

A breach of this size has massive implications. Each device in Orvibo's product catalog can have a different negative effect on its users. This is on top of having an abundance of identifying information about users. Much of the data can be pieced together both to disrupt a person's home while possibly leading to further hacks.

Though Orvibo does hash its passwords, we tested the security ourselves to see how easy it was to discover the real password. In some cases, we uncovered our own password. In order to test this, we created our own account, then searched for our email address to see what account information was accessible. Though our chosen password was hashed, it was easy to crack.

If Orvibo had added salt to their hashed passwords, it would have created a more complex string that is far more difficult to crack. Salt works by adding a random string onto an existing password, which is then hashed. Since the salt is unknown, it becomes very difficult to determine which piece of the password is genuine and which piece was the added string.

This especially highlights why it's so important to choose strong passwords, especially when they're connected to devices with uncertain levels of security.

Even with strong passwords, however, Orvibo's database included a dangerous piece of information. When examining their records, we found account reset codes in the data logs. These would be sent to a user to reset either their password or their email address. With that information readily accessible, a hacker could lock a user out of their account without needing their password. Changing both a password and an email address could make the action irreversible.

There are Orvibo devices whose poor security could have severe consequences. A number of the devices offered by Orvibo fall under the umbrella of "home security." They include smart locks, home security cameras, and full smart home kits. With the information that has leaked, it's clear that there is nothing secure about these devices. Even having one of these devices installed could undermine, rather than enhance, your physical security.

There's enough information leaked from the database that it makes taking over a user's account a simple enough task. A malicious actor could easily access the video feed from one of Orvibo's smart cameras by entering into another user's account with the credentials found in the database. At the same time, it would be easy to unlock a door from the same account. With precise geolocation, this simplifies home break-ins, an event smart homes are supposed to help

protect against.

=====

And Leo, of course this perfectly dovetails on what we were talking about last week... How utterly blind we are to EVERYTHING having to do with this IoT technology.

This is really a big deal. A huge number of people are installing "Internet-connected" networked black boxes all over their homes, pressing a few buttons and "Presto!" -- Look mom, I can check on the dog while I'm visiting. Yeah... And so can someone who may not have your best interests at heart.

The industry has recently been talking about a worm with great concern, so much so that Microsoft has issued repeated warning and both the US's NSA and DHS have done the same. But ALL of those 2+ Billion Orvibo records were created by machine, so they can be read by machine... And acted on instantaneously en mass by machine. If someone in Communist China wished, -- even IF none of Orvibo's products had outright security vulnerabilities, which seems unlikely -- over a million of Orvibo's customers all over the world have invited a potential Trojan horse into their homes, offices and businesses. Perhaps the strategic value of this hasn't occurred to anyone. Or perhaps it has.

With things the way they are now, I'm thinking that IoT should seriously be renamed from "Internet of Things" -to- "Installation of Trojan."

And... Why IS Orvibo logging billions of transaction records for their million+ customers? Why? What's the business purpose for that?

Equally troubling is that vpnMentor has been unable to reach anyone at Orvibo. After eMailing them they posted a note to their Twitter account. No response. No answer. And so this data remains publicly accessible.

~30~