Security Now! #675 - 08-07-18

New WiFi Password Attack

This week on Security Now!

This week we discuss yet another new and diabolical router hack and attack, Reddit's discovery of SMS 2FA failure, WannaCry refuses to die, law enforcement's ample unused forensic resources, a new and very clever BGP-based attack, Windows 10 update dissatisfaction, Google advances their state-sponsored attack notifications, what is Google's project Dragonfly?, a highly effective and highly targeted Ransomware campaign, some closing-the-loop feedback from our listeners, and a breakthrough in hacking/attacking WiFi passwords.

Windows 10 Update / New Feature (Dis)Satisfaction Survey Results:

	1 - VERY MUCH NOT SATISFIED	2 - NOT SATISFIED	3 - NEUTRAL	4 -SOMEWHAT SATISFIED	5 -VERY SATISFIED	TOTAL
Satisfaction with Microsoft patching	31.72% 361	37.26% 424	12.83% 146	15.91% 181	2.28% 26	1,138

	1-VERY MUCH NOT SATISFIED	2-NOT SATISFIED	3-NEUTRAL	4-SOMEWHAT SATISFIED	5-VERY SATISFIED	TOTAL	WEIGHTED AVERAGE
Satisfaction with the quality of Windows 10 updates	32.71% 370	31.56% 357	19.10% 216	13.09% 148	3.54% 40	1,131	2.23

	1-NOT USEFUL AT ALL	2-RARELY USEFUL	3-NEUTRAL	4-SOMEWHAT USEFUL	5-EXTREMELY USEFUL	TOTAL	WEIGHTED AVERAGE
Useful to my business	35.03% 393	34.49% 387	18.81% 211	9.71% 109	1.96% 22	1,122	2.09

	1-ONCE EVERY TWO YEARS	2-ONCE EVERY YEAR	3-NO OPINION	4-TWO TIMES A YEAR IS FINE	5-MORE OFTEN THAN NOW	TOTAL	WEIGHTED AVERAGE
I want feature releases	39.29% 442	39.20% 441	8.89% 100	11.20% 126	1.42% 16	1,125	1.96

Credit: Bleeping Computer - https://www.bleepingcomputer.com/news/microsoft/an-open-letter-to-microsoft-about-poor-windows-10-update-experiences/

Security News

More than 200,000 MikroTik routers infected with crypto mining malware
https://www.trustwave.com/Resources/SpiderLabs-Blog/Mass-MikroTik-Router-Infection-%E2%80%93-First-we-cryptojack-Brazil,-then-we-take-the-World-/

Trustwave / SpiderLabs / Simon Kenin

On July 31st , just after getting back to the office from my talk at RSA Asia 2018 about how cyber criminals use cryptocurrencies for their malicious activities, I noticed a huge surge of CoinHive in Brazil.

After a quick look I saw that this is not your average garden variety website compromise, but that these were all MikroTik network devices.

This could be a bizarre coincidence, but on further inspection I saw that all of these devices were using the same CoinHive sitekey, meaning that they all ultimately mine into the hands of one entity. I looked for the CoinHive site-key used on those devices, and saw that the attacker indeed mainly focused on Brazil.

My first thought was that on such a large scale that could be a zero day exploit, possibly in the MikroTik HttpProxy component, so my next step was to check whether anyone else also noticed this, since during the conference I had limited time and internet access to keep up with daily news.

Google didn't produce many results, but the few that did come up were actually quite useful in helping me pinpoint the attack vector and what the attacker did.

For example, this result show injection of CoinHive on a hospital website in Brazil. However this webserver runs Apache, which contradicted my initial thought of an exploit directly in MikroTik HttpProxy:

After doing some querying on Shodan I actually found the hospital's MikroTik device, so perhaps it is an issue with MikroTik, but not necessarily with the HttpProxy. So there I was, back at square one with a huge surge of CoinHive hits in Brazil but no idea where and how it originated, and back to my Google results I went to see what else they had to offer.

I found a post on Reddit from someone who was repeatedly being infected with CoinHive mining.

</quote>

So it turned out after more digging that the exploit in use was --once again-- not a new 0-day, but exploiting a long since patched and well known vulnerability in MicroTik routers.

It was patched responsibly, one day after it was revealed last April 23rd... yet today, hundreds of thousands of MicroTik routers remain vulnerable.

The exploit targets "Winbox" which is a windows-based management interface offered by the MicroTik routers. And when unpatched is allows attacker full unauthenticated remote admin access to the routers.

However... here's the new and diabolical bit:

Rather than running the CoinHive miner on the router itself, which is how the exploit was being used when it was first discovered, the attacker has since started using the router's intermediate position on its network to DYNAMICALLY INJECT live CoinHive script into every web page that a user visits.

And, this is a bi-directional attack! If the router has publicly accessible servers behind it, OUTGOING pages are also injected with CoinHive script.

Later, fearing that this would expose the router's role, only error pages returned to the router's users would have mining script injections.

Simon finishes his posting by writing:

Let me emphasize how bad this attack is. The attacker wisely thought that instead of infecting small sites with few visitors, or finding sophisticated ways to run malware on end user computers, they would go straight to the source; carrier-grade router devices.

There are hundreds of thousands of these devices around the globe, in use by ISPs and different organizations and businesses, each device serves at least tens if not hundreds of users daily.

Allegedly, each user would have initially gotten the CoinHive script regardless which site they visited. Even if this attack only works on pages that return errors, we're still talking about potentially millions of daily pages for the attacker.

As mentioned, servers that are connected to infected routers would also, in some cases, return an error page with CoinHive to users that are visiting those servers, no matter where on the internet they are visiting from.

Compromised MikroTik customers that have Trustwave SWG connected to the router will see a huge spike in CoinHive blocks.

Stay tuned for possibly more details as we continue to analyze this attack.

(And let's also not forget how much this is benefiting CoinHive, who take a significant piece of the action from the use of their browser scripting.)

Reddit Hacked despite having 2FA in place.
https://www.reddit.com/r/announcements/comments/93qnm5/we_had_a_security_incident_heres_what_you_need_to/

"We had a security incident. Here's what you need to know."

What happened?

On June 19, we learned that between June 14 and June 18, an attacker compromised a few of our employees' accounts with our cloud and source code hosting providers. Already having our primary access points for code and infrastructure behind strong authentication requiring two factor authentication (2FA), we learned that SMS-based authentication is not nearly as secure as we would hope, and the main attack was via SMS intercept. We point this out to encourage everyone here to move to token-based 2FA.

Although this was a serious attack, the attacker did not gain write access to Reddit systems; they gained read-only access to some systems that contained backup data, source code and other logs. They were not able to alter Reddit information, and we have taken steps since the event to further lock down and rotate all production secrets and API keys, and to enhance our logging and monitoring systems.

Emails, Passwords, Private Messages Stolen

If there is any "I forgot my authenticator" bypass...

Speaking of 2FA... Google's Titan security keys.
Yubico / Stina / Chinese / Supply Chain Attacks.

Note: Yubico's very first USB keyboard dongle =was= not static. It was counter-based OTP.

WannyCry (Windows SMBv2) strikes yet again...
And is expected to shave 1/4 billion dollars from a major Taiwanese semiconductor manufacturer as a consequence of multiple manufacturing facilities across three cities being temporarily shutdown.

The company is TSMC (Taiwan Semiconductor Manufacturing Co.). It is not only a major supplier of semiconductor parts to Apple, AMD, Nvidia and Qualcomm... but it's Taiwan's largest company.

TSMC officials wrote: "This virus outbreak occurred due to misoperation during the software installation process for a new tool, which caused a virus to spread once the tool was connected to the company's computer network,"

In statements made yesterday, the officials identified the malware as WannaCry.

The company said it expected the disruption to lower third-quarter revenue by as much as 3 percent. With the chipmaker previously forecasting revenue in the quarter to be $8.45 billion to $8.55 billion, the hit to revenue could be as high as $256 million.

And lets remember that ample evidence points to WannaCry being based upon an advanced NSA exploit named EternalBlue which was originally leaked from the NSA by the Shadow Brokers.

It's unclear why/how WannaCry was able to propagate through TSMC.

Remember that WannaCry was contained by the "kill switch" which security researcher Marcus Hutchins, aka MalwareTech, activated when he registered that special domain name less than a day after the worm was unleashed. He found the unregistered domain embedded in some of the code. After he had registered the domain -- so that DNS queries then began to succeed rather than fail -- he discovered that doing so acted as a switch the attackers could use to terminate the campaign.

The domain's continued existence continues to prevent computers that get exposed to the WannaCry malware from installing a payload that encrypts hard drives and displays a screen demanding a ransom in exchange for a decryption key.

Perhaps inside TSMC, DNS public is blocked or something prevented WannaCry from succeeding with its DNS ping... and so it went to town on their network.

FBI and "The Going Dark" problem...
James Comey's replacement, Christopher Wray, now head of the FBI, is continuing to threaten legislative action if Silicon Valley companies do not offer up some means for responding to a search warrant.

Wray recently said: "I think there should be [room for compromise]. I don't want to characterize private conversations we're having with people in the industry. We're not there yet for sure. And if we can't get there, there may be other remedies, like legislation, that would have to come to bear."

"We're a country that has unbelievable innovation. We put a man on the moon. We have the power of flight. We have autonomous vehicles… [T]he idea that we can't solve this problem as a society -- I just don't buy it."

Bruce Schneier: https://www.schneier.com/blog/archives/2018/07/new_report_on_p.html

New Report on Police Digital Forensics Techniques

CSIS: Center for Strategic & International Studies
https://www.csis.org/analysis/low-hanging-fruit-evidence-based-solutions-digital-evidence-challenge

"Low-Hanging Fruit: Evidence-Based Solutions to the Digital Evidence Challenge"

Over the past year, we conducted a series of interviews with federal, state, and local law enforcement officials, attorneys, service providers, and civil society groups. We also commissioned a survey of law enforcement officers from across the country to better understand the full range of difficulties they are facing in accessing and using digital evidence in their cases. Survey results indicate that accessing data from service providers -- much of which is not encrypted -- is the biggest problem that law enforcement currently faces in leveraging digital evidence.

This is a problem that has not received adequate attention or resources to date. An array of federal and state training centers, crime labs, and other efforts have arisen to help fill the gaps, but they are able to fill only a fraction of the need. And there is no central entity responsible for monitoring these efforts, taking stock of the demand, and providing the assistance needed. The key federal entity with an explicit mission to assist state and local law enforcement with their digital evidence needs -- the National Domestic Communications Assistance Center (NDCAC)has a budget of $11.4 million, spread among several different programs designed to distribute knowledge about service providers' policies and products, develop and share technical tools, and train law enforcement on new services and technologies, among other initiatives.

In addition to bemoaning the lack of guidance and help from tech companies -- a quarter of survey respondents said their top issue was convincing companies to hand over suspects' data -- law enforcement officials also reported receiving barely any digital evidence training. Local police said they'd received only 10 hours of training in the past 12 months; state police received 13 and federal officials received 16. A plurality of respondents said they only received annual training. Only 16 percent said their organizations scheduled training sessions at least twice per year.

</quote>

So... a clear way to read all of this is that while the FBI and other law enforcement agencies are annoyed that they are able to get to everything, they are not nearly making use of everything they CAN already get to.

I'm reminded of the 4 year old at Christmas who is so busy ripping paper off of presents that he or she completely fails to appreciate all the things they have already opened. If there's still one more mystery, no care is given to everything that's already there. The FBI and others are entirely focused upon the one thing they cannot see into... while ignoring so much of use that they can.

Evidence that BGP hijacking is becoming targeted and weaponized.
https://blogs.oracle.com/internetintelligence/bgp-dns-hijacks-target-payment-systems

We recently talked about "Bitcanal", the Portuguese ISP who had, for years, been poisoning BGP by advertising routes to a great many little /24 networks whose IPs it was then reselling/leasing to spammers as a means of avoiding SPAM blacklists.

Now, Oracle writes:

In April 2018, we detailed a brazen BGP hijack of Amazon's authoritative DNS service in order to redirect users of a crypto currency wallet service to a fraudulent website ready to steal their money.

In the past month, we have observed additional BGP hijacks of authoritative DNS servers with a technique similar to what was used in April. This time the targets included US payment processing companies.

As in the Amazon case, these more recent BGP hijacks enabled imposter DNS servers to return forged DNS responses, misdirecting unsuspecting users to malicious sites. By using long TTL values in the forged responses, recursive DNS servers held these bogus DNS entries in their caches long after the BGP hijack had disappeared — maximizing the duration of the attack.

</quote>

Think about how very clever this is...

Misrouting traffic to a payment provider intercepts them for the duration of the BGP attack.

But misrouting traffic to the authoritative DNS server for a payment provider poisons the DNS caches of every non-authoritative DNS server which accesses them during the misrouting.

Oracle Concludes:

"If previous hijacks were shots across the bow, these incidents show the Internet infrastructure is now taking direct hits. Unfortunately, there is no reason not to expect to see more of these types of attacks against the Internet."

An Open Letter to Microsoft About Poor Windows 10 Update Experiences
https://www.bleepingcomputer.com/news/microsoft/an-open-letter-to-microsoft-about-poor-windows-10-update-experiences/

On August 1st, Bleeping Computer's founder, Lawrence Abrams, posted about Susan Bradley, a well-known Microsoft MVP:

Susan Bradley, an 18 year Microsoft MVP focused on Windows patching and patch management, has sent an open letter to Microsoft executives Satya Nadella, Carlos Picoto, and Scott Guthrie about the frustration Windows 10 users have when dealing with installing new updates. This letter includes the results of a survey taken by over 1,000 consultants and over 800 consumers regarding their experience with Windows 10 updates.

Being a Microsoft MVP in Consumer Security, I have known Susan for quite some time and can tell you that she is somewhat of a legend among those who regularly support Microsoft products. When I saw her open letter mentioned at AskWoody.com and posted at ComputerWorld, I read through many of the survey comments and decided to reach out to her to find out more about why she wrote the letter.

"It's due to increasing frustration with patching and patch management issues. I see consultants turning off updates completely as they see that as the only way they can have stable systems I see Server admins saying that Server 2016 is fine except when you want a system that doesn't reboot. I see Surface users get their machines cratered with 1803 side effects with SSD drives." Susan told me via email. "I see more and more people say that waiting to install updates is what one must do. All of these are unacceptable. We can't continue on with the status quo."

Common complaints among the survey respondents are that updates are not reliable, they contain features that most of their users don't need, updates fail to install, updates cause crashes, or updates cause further bugs with installed software. Ultimately, what it comes down to is that many of the comments indicated that installing the constant stream of updates was a risky undertaking and not one taken lightly.

Lawrence followed up two days later, on August 3rd, with a posting on Bleeping Computer: "Microsoft's Poor Reply to Open Letter on Windows 10 Update Experiences" https://www.bleepingcomputer.com/news/microsoft/microsoft-s-poor-reply-to-open-letter-on-windows-10-update-experiences/

It looked as though Susan's reply went into the general population bin and wasn't received by anyone in charge of anything.

G Suite Can Now Alert You of Government-Backed Attacks
https://www.bleepingcomputer.com/news/security/g-suite-can-now-alert-you-of-government-backed-attacks/

Google's longstanding warning to Gail users (since 2012) of apparent state-sponsored attack upon a Gmail user's account has, last week, been extended to Google's for-enterprise G Suite accounts.

Last week Google announced that administrators of G Suite accounts can now enable and configure a special alert when a government-backed cyber-espionage group is trying to hack into one of their company's user accounts.

The new option is available under "Admin Console > Reports > Manage Alerts > Government backed attack" option of the standard G Suite super admin account.

The feature lets admins control what happens inside an organization's G Suite account when a suspected government-backed attack happens:

The G Suite super admin can enable this alert to receive notification of an ongoing government-backed attack and what user account was targeted.

G Suite super admins can also configure automated actions to be taken when such a suspected attack occurs, such as automatically resetting the user's account password.

And the new G Suite alert system lets admins send a copy of the alert to the user, as well, similal to the warnings they usually receive in Gmail.

Google Secretly Planning to Launch a Censored Search Engine in China
https://theintercept.com/2018/08/01/google-china-search-engine-censorship/
https://thehackernews.com/2018/08/censored-google-search-china.html

We've recently been talking about Chinese censorship, Telegram fighting Russia, Apple moving its Chinese user's data into China and handing over control to China's primary government-owned Telecom company, and so on.

Now, according to documents leaked to The Intercept, Google is planning to make a comeback in China with a fully censored search engine with a project known as "Dragonfly".

<quote>

Google is planning to launch a censored version of its search engine in China that will blacklist websites and search terms about human rights, democracy, religion, and peaceful protest, The Intercept can reveal.

The project – code-named Dragonfly – has been underway since spring of last year, and accelerated following a December 2017 meeting between Google's CEO Sundar Pichai and a top Chinese government official, according to internal Google documents and people familiar with the plans.

Teams of programmers and engineers at Google have created a custom Android app, different versions of which have been named "Maotai" and "Longfei." The app has already been demonstrated to the Chinese government; the finalized version could be launched in the next six to nine months, pending approval from Chinese officials.

The planned move represents a dramatic shift in Google's policy on China and will mark the first time in almost a decade that the internet giant has operated its search engine in the country.

Google's search service cannot currently be accessed by most internet users in China because it is blocked by the country's so-called Great Firewall. The app Google is building for China will comply with the country's strict censorship laws, restricting access to content that Xi Jinping's Communist Party regime deems unfavorable.

Within Google, knowledge about Dragonfly has been restricted to just a few hundred members of the internet giant's 88,000-strong workforce, said a source with knowledge of the project. The source spoke to The Intercept on condition of anonymity, as they were not authorized to contact the media. The source said that they had moral and ethical concerns about Google's role in the censorship, which is being planned by a handful of top executives and managers at the company with no public scrutiny.

SamSam Ransomware Attacks Extorted Nearly $6 Million
https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/SamSam-The-Almost-Six-Million-Dollar-Ransomware.pdf

A different approach to Ransomware: Targeted attacks on large companies.

Sophos Report:

As the year 2016 began, a ransomware threat appeared that attacked its victims unlike any previous ransomware attack. SamSam, named after the filename of the earliest sample we uncovered, uses a brutally minimalist, manual approach to target and compromise victims.

The attacker or attackers use a variety of built-in Windows tools to escalate their own privileges, then scan the network for valuable targets. They want credentials whose privileges will let them copy their ransomware payload to every machine – servers, endpoints, or whatever else they can get their hands on.

Once in, the attacker(s) spread a payload laterally across the network; a sleeper cell that lays in wait for instructions to begin encrypting. Ever a predator, the attacker waits until late at night, when the target organization is least well equipped to deal with it, before the final blow is struck. A sneak attack while the target literally sleeps, SamSam encrypts a prioritized list of files and directories
first, and then everything else.

Unlike virtually every other ransomware attack, the entire attack process is manual. No badly worded spam email with an attachment is the culprit. The attacker breaks in the old fashioned way: using tools that attempt as many logins as quickly as the Remote Desktop Protocol will permit, and exploits operating system vulnerabilities, though not as many as you'd think. SamSam usually succeeds when the victim chooses a weak, easily guessed password.

In this report, we'll cover the anatomy of a SamSam attack, and why it isn't necessarily hard to defend against. We also took a deep dive into the ransomware payload, tracing its evolution from an early beta through its (so far) third major revision, with no sign of a slowdown in sight, and an ever-increasing ransom demand with each subsequent attack. Partnering with the cryptocurrency
monitoring firm Neutrino, we traced the money trail and discovered far more victims – and funds – than had been previously reported.

Our researchers have spent so much time on this attack, attacker, and payload, they felt capable of producing a profile of the group behind the attack. The profile precedes an appendix with technical details and IoCs of the attacks.

</quote>

Key Findings

- SamSam has earned its creator(s) more than US$5.9 Million since late 2015.
- 74% of the known victims are based in the United States. Other regions known to have suffered attacks include Canada, the UK, and the Middle East.
- The largest ransom paid by an individual victim, so far, is valued at US$64,000, a significantly large amount compared to most ransomware families.

- Medium- to large public sector organisations in healthcare, education, and government have been targeted by SamSam, but our research discovered that these only make up for about 50% of the total number of identified victims, with the rest comprising a private sector that has remained uncharacteristically quiet about the attacks.

- The attacker uses care in target selection and attack preparation is meticulous. SamSam waits for an opportune moment, typically launching the encryption commands in the middle of the night or the early hours of the morning of the victim's local time zone, when most users and admins would be asleep.

- Unlike most other ransomware, SamSam encrypts not only document files, images, and other personal or work data, but also configuration and data files required to run applications (e.g., Microsoft Office). Victims whose backup strategy only protects the user's documents and files won't be able to recover a machine without reimaging it, first.

- Every subsequent attack shows a progression in sophistication and an increasing awareness by the entity controlling SamSam of operational security.

- The cost victims are charged in ransom has increased dramatically, and the tempo of attacks shows no sign of slowdown

Closing The Loop

Stuart in Seattle
Subject: A flash use case
Date: 01 Aug 2018 08:21:33
:
Long time listener/spinrite user etc. I keep hearing you slam flash. At work we have a use case for flash and as of now there is no work around. We use it to provide a dynamic UI in a PDF file that contains 3D work instructions. It is simply not possible to do this using PDF forms constructs. I agree that for html content flash should go away.

Unfortunately within a PDF file there isn't an alternative at this time. We are in a tricky spot of needing to come up with a different way presenting the work instructions then going through the expensive process of getting the new way certified for production.

Blitz in Phoenix
Subject: you can kill HTTP when you pry it from my cold dead hands
Date: 01 Aug 2018 14:08:03
:
Hey Steve,

<insert Love the show, you guys are great, lots of praise/>

I wanted to bring up one specific scenario where I am actively uncomfortable with HTTPS. When

you join a network and it wants you to accept a terms of service or otherwise authenticate me via a web form. When you try to go to a web site, a captive portal intercepts the connection and returns a page for you to login/agree/whatever. That is fine when the connection is straight up HTTP, cause you can "man in the middle" an HTTP. But when the connection is HTTPS, you get a certificate error. OK, so I could create an exception for that site and NOT store it permanently, but that feels wrong.

In addition, if everyone goes full bore HSTS, doesn't that mean you can no longer bypass a certificate error?

Also, as someone who has to do a lot of network related troubleshooting, I greatly appreciate the ability to turn off SSL during packet captures as it makes it much easier to analyze.

oh, and for anyone who finds themselves hitting a captive portal and they don't want to accept the certificate being presented... try HTTP://neverssl.com . That site is so simple (pronounced "elegant") and straight forward in its design and explanation that I immediately suspected it could be a Steve Gibson creation. I have come to the conclusion that it is not one of yours, but primarily because I would have expected you to mention it at some point if you had created it.

<insert thanks for the show/spinrite/vitaminD info/>

Looking forward to how you handle the 4 digit episode issue (instead of Y2k, would that be the E1K issue?),
Blitz from Phoenix

Cory Bitney in Kalispell, Montana
Subject: Rogue Admin! Help!
Date: 07 Aug 2018 12:03:25
:
Hey Steve,

First of all I am a huge fan of Security Now and SpinRite so thank you for providing both.

The reason I am writing is I am in a bit of a conundrum. I just took over as systems administrator for a new company replacing a sole administrator that initially left the company (after 7 years) on good terms.

At the end of week two I found that he installed crypto-mining software (minergate) on all of the workstations on the domain as well as a few servers. I told the owners and they are concerned but are hesitant to file criminal charges because they have known him so long.

They at least finally gave me permission to do a full lockdown a few days ago and the more I dig the more I find...backdoors, monitoring software, etc. Basically everything in a sys admin's nightmare. He has definitely abused his power.

My question is, if the owners don't press charges do you know of anything I can do to report him? The company he went to work for is an ISP so it scares me to death what he might do with

them. To me someone like this should never be trusted/have a career in IT again! As Uncle Ben said, "With great power comes great responsibility."

Any advice would be greatly appreciated! I know you are a busy person and if I don't hear back it's understandable. Either way thanks again for all your contributions to our industry!

WiFi Password Cracking Breakthrough

https://hashcat.net/forum/thread-7717.html
https://medium.com/@adam.toscher/new-attack-on-wpa-wpa2-using-pmkid-96c3119f7f99

Traditional attack: Requires receiving all four packets passed back and forth between a client and an access point when the client is authenticating.

New attack: Attacker induces a single packet from the AP.

The guy behind Hashcat was poking around at WPA2 & 3 looking for new ways to attack WPA3.

What he found was a new way to attack the WPA2 that everyone is using today!

This attack was discovered accidentally while looking for new ways to attack the new WPA3 security standard. WPA3 will be much harder to attack because of its modern key establishment protocol called "Simultaneous Authentication of Equals" (SAE).

The main difference from existing attacks is that in this attack, capture of a full EAPOL 4-way handshake is not required. The new attack is performed on the RSN IE (Robust Security Network Information Element) of a single EAPOL frame.

At this time, we do not know for which vendors or for how many routers this technique will work, but we think it will work against all 802.11i/p/q/r networks with roaming functions enabled (most modern routers).

The main advantages of this attack are as follow:

- No more regular users required - because the attacker directly communicates with the AP (aka "client-less" attack)
- No more waiting for a complete 4-way handshake between the regular user and the AP
- No more eventual retransmissions of EAPOL frames (which can lead to uncrackable results)
- No more eventual invalid passwords sent by the regular user
- No more lost EAPOL frames when the regular user or the AP is too far away from the attacker
- No more fixing of nonce and replaycounter values required (resulting in slightly higher speeds)
- No more special output format (pcap, hccapx, etc.) - final data will appear as regular hex encoded string

We receive all the data we need in the first EAPOL frame from the AP.

The PMKID is computed by using HMAC-SHA1 where the key is the PMK and the data part is the concatenation of a fixed string label "PMK Name", the access point's MAC address and the station's MAC address.

PMKID = HMAC-SHA1-128(PMK, "PMK Name" | MAC_AP | MAC_STA)