Global Information Assurance Certification Paper

Superfish and TLS: A Case Study of Betrayed Trust and Legal Liability

GIAC GLEG Gold Certification

Author: Sandra Dunn, subzer0girl@gmail.com
Advisor: Adam Kliarsky
Accepted: January, 22nd 2017

Abstract

Superfish, the bloat adware included in Lenovo consumer laptops from 2014-2015 which intentionally broke TLS, exposed user's personal data to compromise and theft, and altered search result ads in user's browsers severely impacted Lenovo brand reputation. There have been other high profile cases of intentionally modifying and breaking TLS that used questionable and deceptive practices but few that generated as much attention and provide such a clear example of a chain of missteps between Lenovo, Superfish, and their customers. A case study of the Superfish mishap exposes the danger, risk, legal liability, and potential government investigation for organization deploying TLS certificates and keys that breaks or weakens the security design and puts private data or people at risk. The Superfish case further demonstrates the importance of a company's disclosure transparency to avoid accusations of deceptive practices if breaking TLS is required to protect users or an organization's data.

1. Introduction

A tweet by Google researcher Chris Palmer brought the Lenovo Superfish catastrophe crashing onto the internet on February 18, 2015. He purchased a Lenovo Yoga 2 after several long Twitter discussions about the strange Lenovo certificate behavior. He discovered certificates for trusted sites such as www.bankofamerica.com signed by an unfamiliar Certificate Authority, Superfish, Inc. His discovery ignited a firestorm of media and watch agency investigation who raised concerns from the severity of the impact to users, to the irresponsible responses from the three companies involved installing the software on the Lenovo consumer computers.

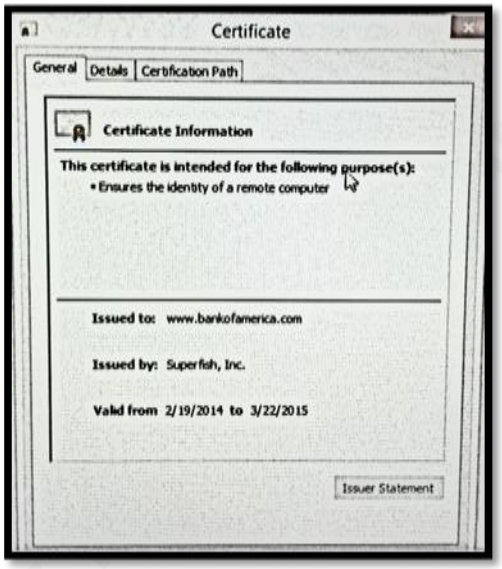

Figure 1 The discovered Superfish certificate

Security researcher Robert Graham, the CEO of Errata Security dove deeper into the discovered certificate, extracting the Superfish certificate and cracking the password for the private key for the installed certificate. He detailed the lack of complexity and the simple steps he used on his blog site, Errata Security. (Graham, Extracting the SuperFish certificate, 2015)

The questions raised by the media and watch groups regarding bloatware, and intentionally breaking TLS certificates implementations were targeted at Lenovo, Superfish, and Komodia but raised difficult to answer question on trust and accountability for all companies that build and deliver software and hardware. For consumers, the Internet was, and is, an ethical wild west. Profits take precedence over ethics and companies are only sorry if they get caught for their misdeeds.

All three of the companies were irresponsible and made un-defendable compromises of their customers' privacy and security, but did they break the law? And whose law was broken? Lenovo, a Chinese company, has a headquarter in the U.S. and

delivers products all over the world. Komodia is an Israeli company. Superfish, was incorporated in the United States but had roots in Israel.

As in the lawless Wild West the cyber frontier has a vigilante swarm, which take the law into their hands when they think the sheriff is failing at keeping the peace in town. In the cyber frontier vigilante swarm voices carry quickly and resonate loudly, especially if a company is abusing or misusing customer's trust and loyalty. Just like a swarm of bees, a swarm of cyber vigilantes gain momentum and power through numbers. The more they are stirred through corporate arrogance, untrue statements, or callous disregard for their customers the more the swarm is stirred into an attacking frenzy. The vigilante swarm can include a wide breadth of members; angry customers, media, attorneys, the U.S. Federal Trade Commission (FTC), state attorney generals, the Electronic Frontier Foundation (EFF), and technical experts who also gain visibility and credibility by detailing front page events in dizzying technical depth.

The most serious criticism of all the three companies involved with the Superfish event, Lenovo, Superfish and Komodia, was targeted at their slow reaction times and initial discounting of the seriousness of the Superfish issue. Classic cyber vigilante swarm fuel.

2. The Superfish Event

Lenovo never fully disclosed their business case for installing the Superfish software on consumer laptops. The media and experts speculate it was an attempt by Lenovo to increase the razor thin margins faced by hardware manufactures. Bundling "bloatware" to increase profits is a common practice for both computer and phone manufactures. Lenovo has steadfastly denied any significant financial benefit for installing the Superfish software and maintained their original statement that the software was included to "Enhance their user's experience" (Lenovo, 2015).

Superfish "enhanced" the Lenovo computer user's experience by recognizing the images on browsed

sites and then presenting similar items in adware based on the returned results visual recognition. Increased use of Transport Layer Security (TLS)[i], the protocol that secures communication with the use of certificates, created a challenge for the Superfish software.

TLS communication between the client browser and the visited site prevented Superfish software from seeing the images the customer was accessing. TLS intercepting libraries from an Israeli company, Komodia, solved this problem. Superfish used the Komodia intercepting libraries to replaces legitimate site certificates with its own Superfish signed certificate and injected its advertisements pulled from a database of images (Fox-Brewster, These Ex-Israeli Surveillance Agents Hijack Your Browser To Profit From Ads, 2015)

Figure 2 Superfish injecting ads in user

The impact to Lenovo / Superfish users is that the security and validation controls for TLS that establish trust were now completely broken leaving them exposed to malicious attacks.

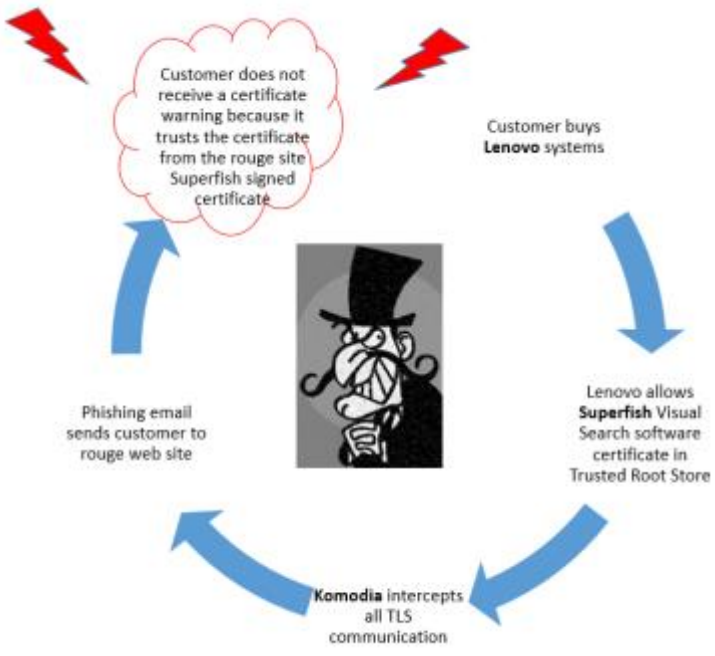

Figure 3 Exploiting Superfish Vulnerability

(1) A customer buys Lenovo system with the Superfish software installed

(2) For any HTTPS enabled website the customer visits a Komodia generated a new certificate for the site signed by the Superfish root certificate.

(3) Komodia libraries intercepts all TLS communication

(4) An attacker cracks the Komodia CA certificate[1] root certificate private key and generates a certificate signed by root certificate and installs it on an imposter website. Attacker sends a phishing email to user that they need to update their banking information and sends them to the imposter site. Since the Webserver certificate is signed by a trusted root certificate that is in the trusted root store of the user, the user does not receive any warning that this is not a legitimate site.

Lenovo had received complaints from customers unhappy with the performance and questioning the Superfish software and what it was doing on their systems (Randune, 2015), but it Chris Palmer's discovery of the Superfish certificate installing itself as a trusted Certificate Authority that ignited the security researcher and media's investigation to learn more about Superfish and how it was implemented on Lenovo computers. Multiple researchers joined the investigation, each uncovering more of the hidden Superfish details and the potential exploitation to Lenovo customers.

Lenovo was the biggest target for most of the customer, media, and security expert's indignation and accountability but the other involved companies were also scrutinized and targeted with eviscerating blog posts and press investigations. Vigilante attackers targeted Lenovo and Komodia's websites with Distributed Denial of Service attacks (DDOS) that took their sites off the internet. In the days following Superfish's discover, Lenovo, Superfish Inc., and Komodia took turns denying the severity of the vulnerability, their individual responsibility, and pointing fingers at the other companies involved.

2.1. Lenovo

People investigating the Superfish issue speculate that Lenovo installed the Superfish software to improve thin profit margins on laptops. Adding bloatware such as Superfish, extra programs used to advertise software, add advertising, or serve a purpose for the manufacturer, is a common practice by hardware manufactures who are looking for any income opportunity to keep their business solvent. Lenovo has repeatedly stated

[1] This is just one attack scenario example where a user could be compromised because of the broken TLS certificate validation.

that the financial benefits were insignificant from the Superfish software or any of the ad related revenue. (Perlroth, 2015) Court documents from Estrella v. Lenovo (CALIFORNIA, 2015), reveal that Superfish Inc. paid Lenovo between $200,000 and $250,000 for including the Superfish software on Lenovo consumer laptops. Lenovo's lack of transparency leaves users open to speculation and conspiracy theories about the Superfish software and who benefit from having access to their private data.

2.2. Superfish Inc.

Superfish Inc. claimed the user benefits for "Enhanced Visual Discovery", improved a Lenovo user's browsing experience by offering the user pop up ads that was similar to images on pages they were browsing. A more accurate description is describing the Superfish software as ad injection software that intercepted the ads on pages visited by the user and replaced them with ads from Superfish's paid advertisers.

Superfish software faced a challenge in delivering their visually modified results. When customers used the encrypted HTTPS protocol the Superfish software was unable to see the images on browsed pages. They came up with a solution, they would get between the encrypted client and server communication with what is referred to as a (MITM) Man in the Middle attack. Superfish Inc. contacted Komodia who offered a variety of solutions designed to intercept encrypted communication.

2.3. Komodia

The Komodia software intercepts the encrypted communication between client and the server. Compare how Komodia works to a person exchanging secrets in a locked briefcase. TLS encrypted traffic by design keeps the secret locked in the briefcase between the two people. Using an interception proxy the secret is instead sent through a third person who locks the secret in his briefcase and throws the original lock away. The original people communicating the secret unaware that their secret communication has been compromised.

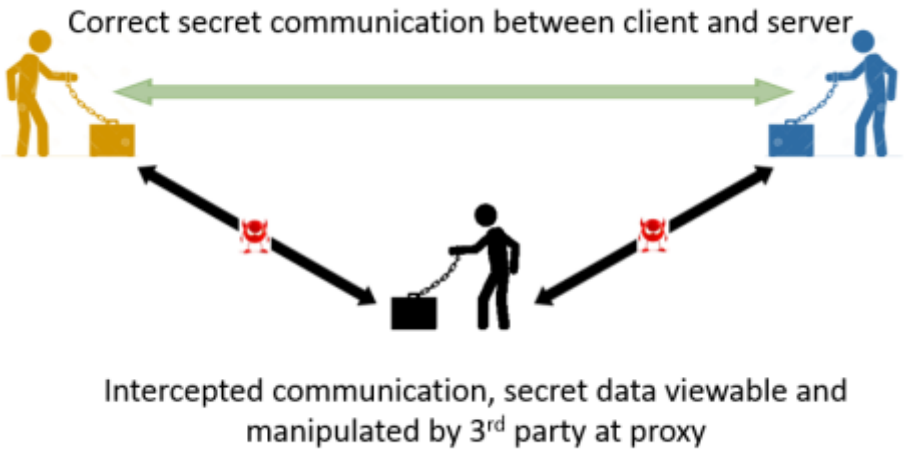

Figure 4 MITM Attack

What made the Komodia implementation especially irresponsible, dangerous, and negligent was that they broke all the security and validation controls for TLS web communication and the Komodia TLS inception framework was used in many other applications beyond Superfish.

As described by Cert Vulnerability Note VU#529496, the Komodia software installs a non-unique root certificate and its private key. The private key for the root certificate which is installed with the Komodia software and protected with a password that was easily crackable. For the Superfish software the password was “komodia” (Graham, Exploiting the Superfish certificate, 2015). The most damaging and dangerous part of Superfish / Komodia managed TLS communication is how Komodia managed an invalid certificates received from a web site that a user browsed to. When Komodia received an invalid certificate it modified the Subject Name on the intercepted root certificate and then signed it with installed root certificate. Signing the certificate with the Superfish root certificate makes the certificate valid since the signature validates against the Superfish root certificate in the root store. Komodia libraries changing the Distinguished name on the web server’s certificate generated browser warning to the users because now the Subject Name in the certificate doesn’tmatch the name in the certificate just signed by the Superfish root certificate. The user receives a browser warning as they should, but it’s done by tricking the protocol instead of providing the

warning because the browser followed the designed TLS protocol process. Unfortunately, this created a bigger security hole for the end user. TLS certificate include another field called the Subject Alternative Field which is used for listing alternate names of sites the certificate can be used to validate a site. The Komodia interception software does not change the domain names in the subject alternative name field so even though the user receives the triggered browsing warning by going to the original subject domain field in the certificate there are no warnings for any of the alternate name fields. Not changing the domain names in the Subject Alternate Field created an ideal opportunity for an attacker to create a rouge site and trick a user into thinking it was a legitimate site, with a legitimate TLS web server certificate. The only thing an attacker would need to do to mascaraed as a legitimate site is generate a certificate that listed the rouge site in the Subject Alternate Field. This attack impacts any site using software the uses Komodia TLS interception libraries (Valsorda, 2015).

In Figure 3 The subject name in the green box is "*.google.com". The subject alternative names highlighted in blue include 47 additional domain names as seen in the blue square that provides details for the Subject Alternative Name field which includes *.google.com, *.android.com *.appengine.google.com *.cloud.google.com*.google-analytics.com *.google.ca etc.

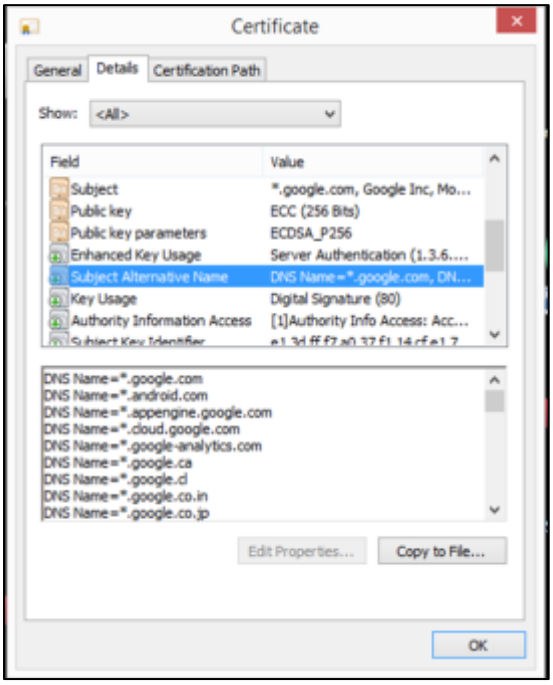

Figure 5 Subject Alternate Names

3. The Swarm

Through social media, individuals, once voiceless and powerless against large corporations now join a vigilante swarm and as a combined force, significantly impact an organization. Angry swarms build energy quickly and start attacking before all the facts are known and using whatever tactics they deem appropriate. The swarm includes wronged individuals, technical experts, protection

groups, government agencies, attorneys, competitors, and attackers looking for supported reasons to gain notoriety.

Top influencers joined the Superfish swarm and engaged 75,328,719 people in 16 days. First they discussed what it was, how bad it was, and then loudly shamed Lenovo, Superfish Inc, and Komodia. In all this negative publicity Lenovo's Twitter account was quiet. There were only six Tweets from the company's @Lenovo account in those first few swarm crazy days, and only one of the tweets responded directly to a customer's direct inquiry (Atkinson & Wittstock, 2015).

3.1. Wronged Individuals

Wronged individuals, often the first members of a swarm, find each other in different way. The most common way they find each other is in a support forum trying to solve the computer problem they have. They compare notes, problem symptoms, and tone deaf responses from an organization. Jessica Bennett, the first person to file a class action law suit against Lenovo, identified her problem through common symptoms other tech forum users were reporting. In the class action lawsuit she filed it states, "Plaintiff searched web forums for help on removing the malicious Spyware on her computer and learned that numerous other consumers were experiencing similar problems with the Superfish product on their recently purchased Lenovo laptop." Case 3:15-cv-00368-CAB-RBB Document 1 Filed 02/19/15. One of those message she read from another Lenovo customer was the catalyst to her realization something beyond standard support issues was happening.

> After doing some research into Superfish Visual Discovery, I consider this software to be quite invasive. It sits between you and whatever sites you visit to monitor your sessions and extract information (it says photos) to serve you advertisements for similar products you may be looking for. What's even more concerning is that it does this for HTTPS connections that the user would expect to be private between themselves and the server they *believe* they are securely connecting to....I have spoken on two separate occasions with Lenovo phone

support, both times they insisted that this Superfish software was not installed by Lenovo and that it is malicious and should be removed, at which time they offered to charge me either a one-time fee of $120, or sell me a monthly software support subscription. I insisted that this Superfish software came pre-installed from the factory, citing where it said "Install Date" in the "Programs and Features" (which was the same install date as the rest of the Lenovo software), as well as the registry entry where Superfish is listed under the "MFGApps" string value. Also, I told them about the folder "Program Files\Lenovo\VisualDiscovery" (if I remember the path name correctly) which used to exist, but I was told this was the virus trying to implant itself somewhere (Randune, 2015)

3.2. Security Researchers / Experts

Security Researchers fuel the vigilante smarm with facts and evidence. They are relied on to discredit any misleading technical claims and provide facts for other parts of the swarm such as attorneys and government agencies. Google researcher Chris Palmer, tweeted the evidence of the Supefish behavior and what he found. He was interviewed and often referenced but refrained from publically bashing Lenovo.

Robert Graham, the first to discuss how he cracked the private key password, also kept to the facts but challenged Lenovo's statement that the attack was theoretical. "Thus, this example proves that this exploit is practical, not merely theoretical as claimed by the Lenovo CTO. Exploiting this was a straightforward application of commonly available tools. The only thing out of the ordinary was sslsplit, but that's a tool commonly used by corporations for security purposes, and not some special "hacking" purpose (Graham, Exploiting the Superfish certificate, 2015) Security researchers Marc Rogers and Filippo Valsorda blog points were openly more poignant.

Marc Rogers's blog on February 19, 2015 stated "We trust our hardware manufacturers to build products that are secure. In this current climate of rising

cybercrime, if you can't trust your hardware manufacturer, you are in a very difficult position. That manufacturer has a huge role to play in keeping you safe – from releasing patches to update software when vulnerabilities are found to behaving in a responsible manner with the data the collect and the privileged access they have to your hardware", "Lenovo has partnered with a company called Superfish to install advertising software on it's customer's laptops. Under normal circumstances, this would not be cause for concern. However, Superfish's software has quite a reputation. It is a notorious piece of "adware", malicious advertising software. A quick search on Google reveals numerous links for pages containing everything from software to remove Superfish to consumers complaining about the presence of this malicious advertising tool. And "This is unbelievably ignorant and reckless of them. It's quite possibly the single worst thing I have seen a manufacturer do to its customer base" (Rogers, 2015).

Filippo Valsorda stated "This is catastrophic", and "Komodia should be punished for jeopardizing the users, like probably all the companies that didn't do due diligence here (Valsorda, 2015).

3.3. Consumer Protection Groups

Consumer protection groups join the swarm to protect consumers and ensure companies provide accurate information. Many protection groups are associated with government agencies but some like the EFF are donor funded non-profit and challenge digital rights abuse by both government and business.

3.3.1. EFF

When the voice of the EFF joins the swarm it has a booming impact across the internet. Their mission is to defend civil liberties in the digital world. Armed with their lawyers, an independent agenda, and their research group, they hold organizations accountable for events that damage individual's privacy or put users at risk. They condemned the Superfish software behavior with a strong statement "Lenovo has not just injected ads in a wildly inappropriate manner, but engineered a massive security catastrophe for its users" (Bonneau, Eckersley, & Hoffman-Andrews, 2015). The EFF was already concerned about the state of TLS and had created the Decentralized SSL Observatory, a project to investigate how certificates are used to secure all of the sites

encrypted with HTTPS on the Web. After the Superfish event was exposed they quickly searched the database and then reported, "...the Decentralized SSL Observatory has seen 44,000 Superfish MITM certificates, all of which have been signed by the same Superfish root cert" (Bonneau, Eckersley, & Hoffman-Andrews, 2015). The EFF posted detailed instructions on how to remove the Superfish software and the offending Superfish certificate on their website (Kamdar, 2015).

3.3.2. Attorney Generals

State Attorney Generals join the Swarm because of a genuine concern for consumers and to increase their public exposure, often fueled by future polical ambitions. A state attorney provides counsel to their state legislature and agencies. They have the power to initiate investigations into organizations where there is evidence of deceptive advertising, public corruption, consumer abuses, or securities violations. In the Lenovo Superfish event the only State Attorney who launched an investigation was Connecticut's George Jepsen (Attorney General George Jepsen, 2015).

3.3.3. FTC

The Federal Trade Commission (FTC) is an independent U.S. Government agency whose primary mission is consumer protection and the prevention of anticompetitive business practices. Often a formidable foe when a company is accused of poor practices it did not launch a formal investigation but did provide a warning on its site with instructions on how to remove the Superfish software (Jhaveri, 2015).

3.3.4. US Cert / Homeland Security

The US Cert issued a high vulnerability warning of 8.4 for the Superfish / Komodia software VU#529496 on February 20, 2015. The US Cert vulnerability notification officially validated the Superfish issue and gained the attention of CISO's and information security professionals. They join the swarm by using their relationships and buying power to put pressure on the offending organization. Lenovo stated they Superfish was only included on consumer laptops, but it raised questions on their software practices across their organizations (US-CERT, 2015).

3.4. Attorneys

Opportunistic and financially motivated attorney's join the swarm urging wronged individuals to join in a class action lawsuit. This usually nets the user very little money but can be a financial wind fall for the attorney's. Many law firms announced the pursuit of a Class Action lawsuit against Lenovo and Superfish Inc. These included Keller, Rohrback L.L.P., The Rosen Law Firm, and Weitz & Luxenberg.

In Business Wire articles announcing the different Superfish lawsuits, the articles included a prepopulated tweet. A user simply clicked and immediately their voice was part of the smarm, announcing their Superfish and Lenovo indignation to their Twitter followers (Business Wire, 2015) (Business Wire, 2015) (Business Wire, 2015).

Figure 6 Tweets from Business Wire Page

3.5. Competitors

In any fierce competitive environment, one company's disaster is another company's opportunity to win over customers. Cool headed marketing departments normally use subtle techniques to leverage swarm events, highlighting how they prevent such issues without directly naming a competitor but not always. Hewlett-Packard was scathingly reproached for a tweet from HP's Twitter account sent on February 20, 2015 which sang "The only thing you should have to think of when someone says Superfish" and attached a picture of Sushi. The tweet was blamed on a misguided outside marketing firm and

quickly removed but HP found themselves apologizing and responding to their wave of negative customer feedback (Matyszczyk, 2015).

Dell's jab was more indirect, only commenting that if customers' were concerned about privacy and Superfish Dell had a better solution. Their subtle was something they were likely thankful for when they faced their certificate event a few months later which the media dubbed "Superfish 2.0" (Jennings, 2015).

3.6. The Attacker

The Attacker is one of the most dangerous swarm members. The attacker swarm includes both idealists who view hacking as an opportunity for positive social disobedience and the bad attacker who is looking for an opportunity to be destructive with reason.

In the Superfish incident, Lenovo and Komodia's websites endured swarm attacker DDOS attacks after Superfish was exposed. The DDOS briefly impacted the Lenovo site but the Komodia site was down for several days. The Lizard Squad claimed that they had also compromised Lenovo's systems and accessed Superfish emails but fell short of proving such a feat (Fox-Brewster, Lizard Squad Claims To Have Intercepted Lenovo Emails After Website Defacement, 2015).

4. Addressing the Swarm

The Superfish incident taught a hard lesson Lenovo, Superfish, and Komodia on managing the swarm. In the SANS LEG523 course, written and taught by Mr. Wright, managing the swarm requires humble transparency, taking ownership, offering swift resolution, fair compensation, and future prevention strategies to them (Wright, 2016). Responsive and responsible organizations, placates the swarm and deflates their momentum. The swarm then dissipates until the next swarm worthy event. Neither Lenovo nor Superfish Inc. practiced good swarm management as reflected in their initial responses.

Lenovo's first official Superfish response deflected responsibly and generated a media backlash. It was taken down from their site within hours. The tone of the statement was unapologetic, it attacked the media and people investigating the issue, and it further

colored Lenovo as ill-informed about the Superfish software, claiming that extensive testing had been completed and no issues had been discovered.

"There has been significant misinformation circulating about Superfish software that was pre-installed on certain Lenovo laptops…Despite the false and misleading statements made by some media commentators and bloggers, the Superfish software does not present a security risk… Superfish takes great pride in the quality of its software, the transparency of its business practices, and its strong relationship with the Superfish user community" (Anderson, 2015)

Lenovo's replacement official statement was significantly more apologetic although they maintained that Superfish software was installed to improve the customer's experience.

> RESEARCH TRIANGLE PARK, NC – February 19, 2015: At Lenovo, we make every effort to provide a great user experience for our customers. We know that millions of people rely on our devices every day, and it is our responsibility to deliver quality, reliability, innovation and security to each and every customer. In our effort to enhance our user experience, we pre-installed a piece of third-party software, Superfish (based in Palo Alto, CA), on some of our consumer notebooks. The goal was to improve the shopping experience using their visual discovery techniques (Lenovo, 2015).

In an interview with the Wall Street Journal on February 19, 2015 Lenovo's chief technology officer, Peter Hortensius, acknowledged Lenovo's responsibility."We didn't do enough due diligence" He then stated,"We're not trying to get into an argument with the security guys. They're dealing with theoretical concerns. We have no insight that anything nefarious has occurred (Ovide, 2015). Mr. Hortensisus Wall Street Journal interview fueled the swarm into a frenzy with researchers such as Robert Graham quickly discrediting the "theoretical" statement and adding evidence to Lenovo's already tarnished reputation.

Sandra (Sandy) Dunn subzer0girl@gmail.com

In an interview with PCWorld the next day Mr. Hortensius recanted on his statements made the previous day stating, “At the end of the day, we’re seeing clearly that we messed up,” This admission of misconduct is in the court filing case summary (Hachman, 2015).

Mr. Horensius released a Superfish Update – An Open Letter From Lenovo CTO Peter Hortensius, on February 23. Lenovo also released a third public statement on February 27, 2015 that promised a cleaner, safer PC. It was too little too late, neither statements generated momentum or a positive response in the swarm community. (Lenovo, 2015) (Lenovo, 2015).

4.1. Superfish Inc.

Superfish’s CEO, Adi Pinahs, only statement to the press insisted his company was not at fault and implicated Komodia as the organization who failed customers and introduced the vulnerability. Dan Goodin, a respected tech writer, points out this shirking of responsibility was a customer relationship failure by Superfish Inc. Dan Goodin wrote, “Superfish doubles down, says HTTPS-busting adware poses no security risk…That's too bad. The CEO had a chance to regain the trust of some people by providing a detailed autopsy that explained how software with his company's name on it put so many Lenovo users at risk. This missed opportunity may make it impossible for him to repair the damage now” (Goodin, 2015). This comment was a prophesizing point. Both Superfish Inc. and Mr. Pinahs next business, JustVisual both closing down their operation of business.

4.2. Komodia

It was the Komodia the SSL hijacker and SSL decrypter libraries that did the interception of the TLS communication and made the interception of the TLS communication possible. Programmer, Barak Weichselbaum developed Komodia. Komodia was not named in any lawsuits and did not offer any public statement regarding their involvement in Superfish.

In a Slate article on February 24, 2015, author David Auerbach, states that Komodia is more incompetent than evil and put the responsibility for Superfish on Lenovo and Superfish Inc (Auerbach, 2015).

5. The Legal case against Lenovo and Superfish Inc.

In spite of all the backlash and accusations Lenovo and Superfish faced little Federal or state investigation. The State Attorney of Connecticut, George Jepsen sent letters of investigation to both Lenovo and Superfish. There is no information that indicates there was a formal suit resulting from this initial investigation. The FTC did not launch a formal investigation.

On February 19th, Jessica Bennett filed the first lawsuit against Lenovo and Superfish, which was quickly followed by 28 other suites in 33 states. In June 2015, the 28 filed cases were combined into a consolidated case: Lenovo Adware Litigation, No. 5:15-cv-02624 and sent to the U.S. District Court for the Northern District of California. In the consolidated case the parties agreed to narrow the scope and only proceed under Federal, New York, and California law. The consolidated cased named six plaintiffs who listed twelve causes of actions against Lenovo based on the following allegations:

- Violation of Computer Fraud and Abuse Act
- Violation of the Electronic Communications Privacy Act; 1
- Violation of the California's Unfair Competition Law;
- Violation of California's Consumer Legal Remedies Act;
- Violation of California's Computer Crime Law;
- Violation of California's Consumer Protection Against Computer Spyware Act;
- Violation of California's Invasion of Privacy Act;
- Negligence under California law;
- Trespass to chattels under California law;
- Violation of New York's Deceptive Acts & Practice;
- Negligence under New York law; and
- Trespass to chattels under New York law

Sandra (Sandy) Dunn subzer0girl@gmail.com

On February 11, 2016, Superfish Inc. settled the privacy case against them for $1 Million dollars, And promised to assist the plaintiffs in their continued lawsuit against Lenovo, by giving the plaintiffs access to over 2.8 million additional files and providing Superfish witnesses for a potential trial (Kakuk, 2016)

On October 27, 2016 Judge U.S. District Judge Ronald M. Whyte dismissed many of the claims brought on Lenovo but allowed the plaintiffs to move forward with seven of the actions. These included alleged violations of the Computer Fraud and Abuse Act and California's Computer Crime Law, Unfair Competition Law and Consumer Legal Remedies Act. As of January, 2017 the Lenovo has not settled the case against them (United States District Court Northern District of California San Jose Division, 2016).

5.1. Financial Impact

In the backlash and volume of negative publicity, many bloggers and users predicted a Superfish financial disaster but stock and pc volumes are unable to support this claim. Lenovo's stock price was already on a steep decline before the Superfish event and a financial article published three months after Superfish did not name the Superfish event as one of the reasons for the stock decline. Instead it cited reduced demand for personal computers and Lenovo's poor smart phone strategy. Charles Arthur, a technology writer for "The Guardian" actually predicted a positive financial outcome for Lenovo because of the negative view on bloatware, driving smaller pc manufactures out of the market since they needed to include bloatware to be profitable. IDC numbers from 2005 until 2016 show an increased revenu dollar for 2015 (IDC, 2017) .

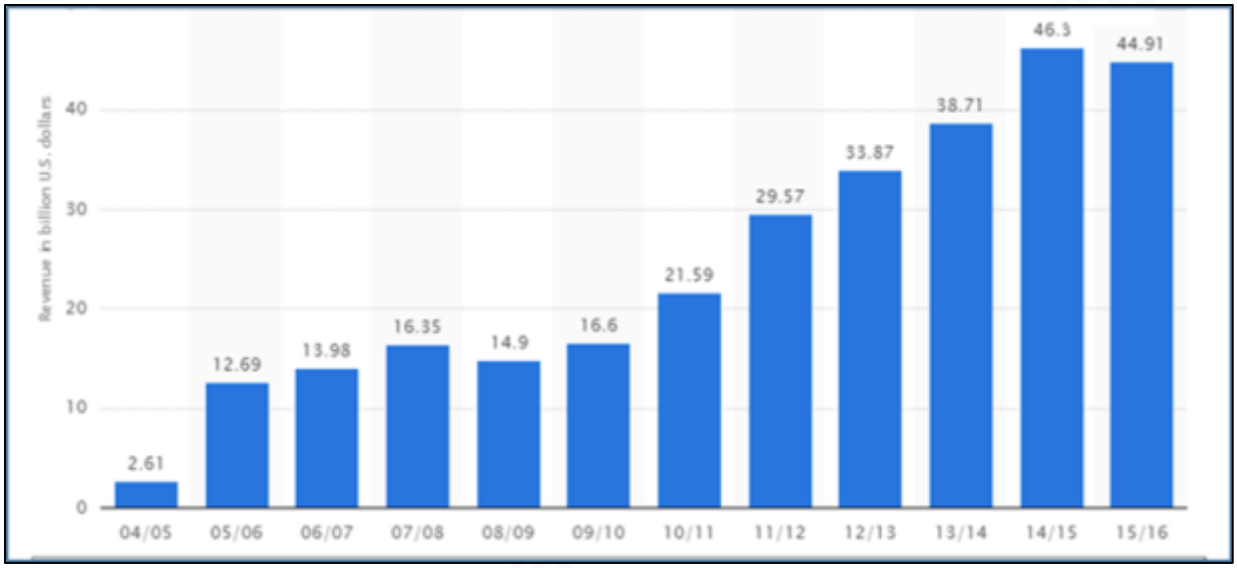

Figure 7 Lenovo Revenue 2005-2016

Fourth quarter worldwide shipments of Lenovo's did decline 4.5 %, but declined less than their two main competitors, HP, who declined 10.1 %, and Dell who declined 5.7 % (Statista, 2017).

Top 5 Vendors, Worldwide PC Shipments, Fourth Quarter 2015 (Preliminary)

(Shipments are in thousands of units)

Vendor	4Q15 Shipments	4Q15 Market Share	4Q14 Shipments	4Q14 Market Share	4Q15/4Q14 Growth
1. Lenovo	15,394	21.4%	16,125	20.0%	-4.5%
2. HP	14,290	19.9%	15,900	19.8%	-10.1%
3. Dell	10,169	14.1%	10,780	13.4%	-5.7%

Figure 8 Lenovo, HP, Dell, Shipment Growth

5.2. Superfish

Superfish Inc. company shut down operations within a few months of the Lenovo Superfish incident although it appears that it was more of a rebranding then a change in strategy. In May of 2015, 3 months after the debacle Superfish's co-founder, Adi Pinahs moved his resources to a new company "JustVisual" which also ceased operations in September of 2016 (Ducklin, 2015).

Sandra (Sandy) Dunn subzer0girl@gmail.com

5.3. Komodia

Komodia still offers SSL Digestor on its website, and continue to describe it as a SSL hijacker. Customers continue to complain about what it does on their system. They describe the Komodia software as malware, a virus, and a rootkit (MyPCgotaRootKit, 2016).

6. Postmortem

The Superfish event provides important lessons for both hardware and software providers. Customers have an amplified voice through the swarm. The previous large organization strategy of ignoring individual complaints, communicating to press inquiries with silence, no comment, or inaccurate statements is taken as contempt, poor customer care, or ineptness. If Lenovo's support team had addressed their customer's initial concerns, performed a proper investigation into the strange reported software behavior, and responsibly provided a security update and removal tool, its possible this event would not have gained the attention and notoriety that it did. There were multiple opportunities for Lenovo to address the swarm and remediate the issue, but by the time Lenovo and their CTO provided a customer and security researcher friendly response, it was too little, too late.

Lenovo had already been identified as a possible security concern by the US Government before the Superfish incident so it's possible that the financial implications of losing untrusting US government and corporate US business had already happened. The people who care about security had already transitioned to a different vendor (Nash, 2017). The FTC did not pursue a case against Lenovo but in the 24 months since the Lenovo case the FTC has focused more scrutiny and lawsuits on companies that sell products with security vulnerabilities (Security Ledger, 2017).

7. Conclusion

Whether intentionally breaking TLS is unlawful is still an open question. Superfish Inc. settled their case for breaking privacy laws but there was no charge brought against them for knowingly modifying how a security protocol works (Got A Class Action, 2016). The case against Lenovo is still open but none of the remaining actions address the intentional breaking of the TLS protocol (Corporate Counsel , 2017). Modifying and manipulating the validation and communication of TLS encrypted communication is still a common practice with software solutions (Carnavalet & Mannan, 2016) and continues to be expose consumers to possible exploitation (ISSA, 2017).

Technology users care about security and they have a voice through a swarm. Although the data does not support a direct impact to Lenovo's stock price due to the Superfish issue, they have been unable to rebuild a reputation as company that delivers a secure product as evidenced in recent Twitter activity.

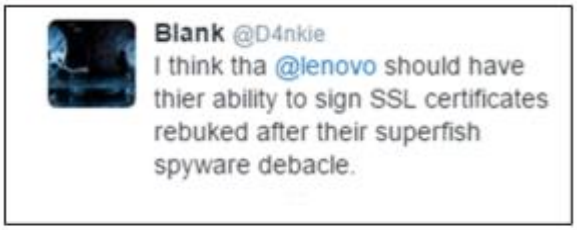

Figure 9 Tweet 1.9.2017

Lenovo is investing and actively addressing customers' security concerns and publishing their product security strategy (Lenovo, 2016). In the two years since the Superfish event organizations have faced increased scrutiny, pressure, trust accountability, and repercussions from agencies such as the EFF and the FTC. It's possible that if the Superfish event happened in today's internet, lawsuits would be even more actively pursued and for higher financial claims.

The power of the swarm watch organizations provides extra incentive Software and hardware manufactures to implement a secure development cycle and to do their best to create security sound products. As an organization keep what the FTC is doing in your sights and be ready to defend practices and decisions.

Sandra (Sandy) Dunn subzer0girl@gmail.com

References

Anderson, N. (2015, February 19). Lenovo honestly thought you'd enjoy that Superfish HTTPS spyware. Retrieved January 13, 2017, from http://arstechnica.com/security/2015/02/lenovo-honestly-thought-youd-enjoy-that-superfish-https-spyware/

Atkinson, C., & Wittstock, M. (2015, December 10). Lenovo: Fame to Shame over Superfish. Retrieved January 12, 2017, from https://verifeed.com/lenovo-fame-to-shame-over-superfish/

Attorney General George Jepsen. (2015, March 2). AG Jepsen Opens Inquiry into Lenovo, Superfish Privacy and Security Concerns. Retrieved January 12, 2017, from http://www.ct.gov/ag/cwp/view.asp?Q=561648&A=2341

Auerbach, D. (2015, February 24). Are Lenovo and Superfish Evil or Incompetent. Retrieved January 12, 2017, from http://www.slate.com/articles/technology/bitwise/2015/02/lenovo_superfish_scandal_the_result_of_evil_or_incompetence.html

Bonneau, J., Eckersley, P., & Hoffman-Andrews, J. (2015, February 19). Lenovo Is Breaking HTTPS Security on its Recent Laptops. Retrieved January 12, 2017, from https://www.eff.org/deeplinks/2015/02/further-evidence-lenovo-breaking-https-security-its-laptops

Business Wire. (2015, February 20). CONSUMER COMPUTER SECURITY ALERT: The Rosen Law Firm Advises Consumers to Take Steps to Remove Adware from Lenovo Computers Purchased between September 2014 Through January 2015. Retrieved January 12, 2017, from http://www.businesswire.com/news/home/20150220005737/en/CONSUMER-COMPUTER-SECURITY-ALERT-Rosen-Law-Firm

Business Wire. (2015, February 19). Keller Rohrback L.L.P. Investigating Superfish Adware on Lenovo Computers. Retrieved January 12, 2017, from http://www.businesswire.com/multimedia/home/20150219006362/en/

Business Wire. (2015, March 16). Weitz & Luxenberg Files Class-Action Against Lenovo, Superfish. Retrieved January 12, 2017, from

Sandra (Sandy) Dunn subzer0girl@gmail.com

http://www.businesswire.com/news/home/20150316006168/en/Weitz-Luxenberg-Files-Class-Action-Lenovo-Superfish

CALIFORNIA, U. S. (2015, 5 March). Rhonda Estrella et al v. Lenovo (United States) Inc. et al, No. 5:2015cv01044 - Document 14 (N.D. Cal. 2015). Retrieved January 10, 2017, from http://www.hodgsonruss.com/media/publication/793_AFD%20the%20Bulletin%205%2015.pdf

Carnavalet, X. d., & Mannan, M. (2016, February 12). Killed by Proxy: Analyzing Client-end TLS Interception Software. Montreal, Quebec, Canada. Retrieved January 12, 2017, from https://www.internetsociety.org/sites/default/files/blogs-media/killed-proxy-analyzing-client-end-tls-interception-software.pdf

Corporate Counsel . (2017, January). Deals & Suits. Retrieved January 12, 2017, from http://www.corpcounsel-digital.com/corpcounsel/sample?search_term=superfish&search_term=superfish&pg=31#pg31

Ducklin, P. (2015, February 20). Lenovo "Superfish" controversy - what you need to know. Retrieved January 13, 2017, from https://nakedsecurity.sophos.com/2015/02/20/the-lenovo-superfish-controversy-what-you-need-to-know/

Fox-Brewster, T. (2015, February 25). Lizard Squad Claims To Have Intercepted Lenovo Emails After Website Defacement. Retrieved January 12, 2017, from http://www.forbes.com/sites/thomasbrewster/2015/02/25/lizard-squad-claims-to-have-access-to-lenovo-emails-after-website-defacement/#8dae84a6822e

Fox-Brewster, T. (2015, January 9). These Ex-Israeli Surveillance Agents Hijack Your Browser To Profit From Ads. Retrieved January 12, 2017, from These Ex-Israeli Surveillance Agents Hijack Your Browser To Profit From Ads

Goodin, D. (2015, February 20). Superfish doubles down, says HTTPS-busting adware poses no security risk. Retrieved January 12, 2017, from

http://arstechnica.com/security/2015/02/superfish-doubles-down-says-https-busting-adware-poses-no-security-risk/

Got A Class Action. (2016, Febrary 13). Superfish agrees to pay $1 million to settle a class-action privacy lawsuit. Retrieved 1 12, 2017, from http://gotaclassaction.com/superfish-agrees-to-pay-1-million-to-settle-a-class-action-privacy-lawsuit/

Graham, R. (2015, February 21). Exploiting the Superfish certificate. Retrieved January 12, 2017, from http://blog.erratasec.com/2015/02/exploiting-superfish-certificate.html#.WHflLVMrJaR

Graham, R. (2015, February 19). Extracting the SuperFish certificate. Retrieved January 10, 2017, from http://blog.erratasec.com/2015/02/extracting-superfish-certificate.html#.WHUGklMrLmF

Hachman, M. (2015, February 20). Lenovo CTO admits company 'messed up,' publishes Superfish removal tool. Retrieved January 12, 2017, from http://www.pcworld.com/article/2886690/lenovo-cto-admits-company-messed-up-and-will-publish-superfish-removal-tool-on-friday.html

IDC. (2017, January 6). PC Market Finishes 2015 As Expected, Hopefully Setting the Stage for a More Stable Future, According to IDC . Retrieved January 6, 2017, from https://www.idc.com/getdoc.jsp?containerId=prUS40909316

ISSA. (2017, January 5). Kaspersky Fixes Two Certificate Flaws. Retrieved January 12, 2017, from http://www.isssource.com/kaspersky-fixes-two-certificate-flaws/

Jennings, R. (2015, November 24). Dell Danger! “Superfish 2.0” blunder: It gets worse. Retrieved January 12, 2017, from http://www.computerworld.com/article/3008219/security/dell-edellroot-laptops-superfish-itbwcw.html

Jhaveri, A. (2015, February 27). Superfish software on Lenovo notebooks: What you can do. Retrieved January 12, 2017, from https://www.consumer.ftc.gov/blog/superfish-software-lenovo-notebooks-what-you-can-do

Sandra (Sandy) Dunn subzer0girl@gmail.com

Kakuk, M. A. (2016, February 16). Lenovo Spyware Defendant Superfish Settles for $1 Million. Retrieved January 12, 2017, from https://topclassactions.com/lawsuit-settlements/lawsuit-news/328327-lenovo-spyware-defendant-superfish-settles-1-million/

Kamdar, a. (2015, February 19). How to Remove Superfish Adware From Your Lenovo Computer. Retrieved January 12, 2017, from https://www.eff.org/deeplinks/2015/02/how-remove-superfish-adware-your-lenovo-computer

Lenovo. (2015, February 19). Retrieved January 10, 2017, from http://news.lenovo.com/news-releases/lenovo-statement-on-superfish.htm

Lenovo. (2015, February 20). LENOVO'S PROMISE FOR A CLEANER, SAFER PC. Retrieved January 12, 2017, from http://news.lenovo.com/article_display.cfm?article_id=1934

Lenovo. (2015, February 23). SUPERFISH UPDATE - AN OPEN LETTER FROM LENOVO CTO PETER HORTENSIUS. Retrieved January 12, 2017, from http://news.lenovo.com/article_display.cfm?article_id=1932

Lenovo. (2016, May 9). Lenovo's Product Security Strategy. Retrieved January 12, 2017, from http://s3.amazonaws.com/isby/lenovopartnernetwork.com/upload/4/docs/Accelerate-2016-Lenovo-Product-Security-Strategy-Presentation.pdf

Matyszczyk, C. (2015, February 21). HP sneers at Lenovo's Superfish problems. Retrieved January 12, 2017, from https://www.cnet.com/news/hp-sneers-at-lenovos-superfish-problems/

MyPCgotaRootKit. (2016, March 16). Komodia Rootkit help. Retrieved January 12, 2017, from https://www.bleepingcomputer.com/forums/t/608495/komodia-rootkit-help/

Nash, C. (2017, 12 1). Report: Pentagon Warns Against Use of Lenovo Computers over Chinese Spyware. Retrieved from http://www.breitbart.com/tech/2016/10/24/report-pentagon-warns-against-use-of-lenovo-computers-over-chinese-spyware/

Sandra (Sandy) Dunn subzer0girl@gmail.com

Ovide, S. (2015, February 19). Lenovo CTO: We're Working to Wipe Superfish App Off of PCs. Retrieved January 12, 2017, from http://blogs.wsj.com/digits/2015/02/19/lenovo-cto-were-working-to-wipe-superfish-app-off-of-pcs/

Perlroth, N. (2015, March 1). How Superfish's Security-Compromising Adware Came to Inhabit Lenovo's PCs. Retrieved January 10, 2017, from https://www.nytimes.com/2015/03/02/technology/how-superfishs-security-compromising-adware-came-to-inhabit-lenovos-pcs.html?_r=0

Randune. (2015, 1 30). Pre-installed Superfish Visual Discovery on Lenovoe Flex 2-15. Retrieved January 10, 2017, from https://forums.lenovo.com/t5/Lenovo-IdeaPad-100-305-500-Edge/Pre-installed-Superfish-Visual-Discovery-on-Lenovo-Flex-2-15/td-p/1896989

Rogers, M. (2015, 19 February). Lenovo installs adware on customer laptops and compromises ALL SSL. Retrieved January 12, 2017, from http://marcrogers.org/2015/02/19/lenovo-installs-adware-on-customer-laptops-and-compromises-all-ssl/

Security Ledger. (2017, January 6). FTC Sues D-Link Citing Security Flaws in Routers, Cameras. Retrieved January 12, 2017, from https://securityledger.com/2017/01/ftc-sues-d-link-citing-security-flaws-in-routers-cameras/

Statista. (2017, January 6). Revenue of Lenovo from 2004/05 to 2015/16 (in billion U.S. dollars). Retrieved January 6, 2017, from https://www.statista.com/statistics/233035/revenue-of-lenovo/

United States District Court Northern District of California San Jose Division. (2016, October 27). Case 5:15-md-02624-RMW. Retrieved January 12, 2017, from http://pdfserver.amlaw.com/ca/LenovoMTDOrder.pdf

US-CERT. (2015, February 20). Lenovo Computers Vulnerable to HTTPS Spoofing. Retrieved January 12, 2017, from https://www.us-cert.gov/ncas/current-activity/2015/02/20/Lenovo-Computers-Vulnerable-HTTPS-Spoofing

Sandra (Sandy) Dunn subzer0girl@gmail.com

Valsorda, F. (2015, February 15). Komodia/Superfish SSL Validation is Broken. Retrieved January 12, 2017, from https://blog.filippo.io/komodia-superfish-ssl-validation-is-broken/

Wright, B. (2016). *LEG523: Applying Law to Emerging Dangers: Cyber Defense.* Maryland, USA: The SANS Institute.

Sandra (Sandy) Dunn subzer0girl@gmail.com

[i] See these papers for additional details on TLS and certificates

- The Scary and Terrible Code Signing Problem You Don't Know You Have https://www.sans.org/reading-room/whitepapers/critical/scary-terrible-code-signing-problem-you-36382
- The Business Case for TLS Certificate Enterprise Key Management of Web Site Certificates: Wrangling TLS Certificates on the Wild Web https://www.sans.org/reading-room/whitepapers/critical/business-case-tls-certificate-enterprise-key-management-web-site-certificates-wrangling-36392
- Defending Against the Weaponization of Trust: Defense in Depth Assessment of TLS https://www.sans.org/reading-room/whitepapers/auditing/defending-weaponization-trust-defense-in-depth-assessment-tls-37145

Sandra (Sandy) Dunn subzer0girl@gmail.com