# The hunt for the dawn of APTs

**DUBAI:** Kaspersky Lab and Kings College London researchers, looking for a link between a modern threat actor and the Moonlight Maze attacks that targeted the Pentagon, NASA and more in the late 1990s, have unearthed samples, logs and artefacts belonging to the ancient APT. The findings show that a backdoor used in 1998 by Moonlight Maze to tunnel information out of victim networks connects to a backdoor used by Turla in 2011 and possibly as recently as 2017.

If the link between Turla and Moonlight Maze is proven, it would place the evolved threat actor alongside theEquation Group in terms of its longevity, as some of Equation's command-and-control servers date back to 1996. Contemporary reports on Moonlight Maze show how, starting from 1996, US military and government networks, as well as universities, research institutions and even the Department of Energy began detecting breaches in their systems.

In 1998, the FBI and the Department of Defense launched a massive investigation. The story became public in 1999, but much of the evidence has remained classified, leaving the details of Moonlight Maze shrouded in myth and secrecy. Over the years, original investigators in three different countries have stated that Moonlight Maze evolved into Turla, a Russian-speaking threat actor also known as Snake, Uroburos, Venomous Bear, and Krypton. Turla is conventionally believed to have been active since 2007.

### Cupboard Samples

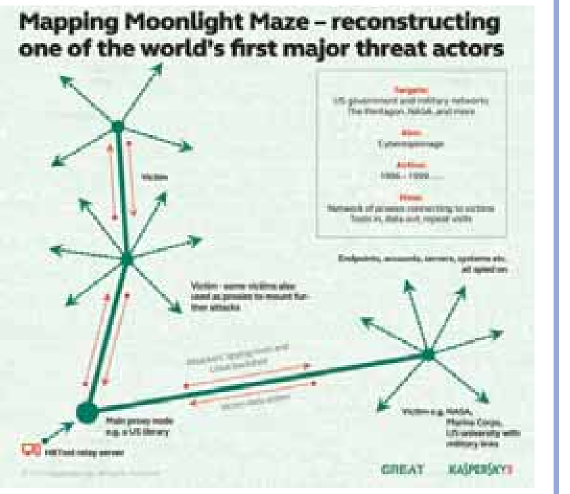
In 2016, while researching his book, Rise of the Machines, Thomas Rid of Kings College London tracked down a former system administrator whose organization's server had been hijacked as a proxy by the Moonlight Maze attackers. This server, 'HRTest', had been used to launch attacks on the US. The now-retired IT professional had kept the original server and copies of everything relating to the attacks, and handed it to Kings College and Kaspersky Lab for further analysis.

Kaspersky Lab researchers, Juan Andres Guerrero-Saade and CostinRaiu, together with Thomas Rid and Danny Moore from Kings College, spent nine months undertaking a detailed technical analysis of these samples. They reconstructed the attackers' operations, tools, and techniques, and conducted a parallel investigation to see if they could prove the claimed connection with Turla.

Moonlight Maze was an open-source Unix-based attack targeting Solaris systems, and the findings show that it made use of a backdoor based on LOKI2 (a program released in 1996that enables users toextract data via covert channels). This led the researchers to take a second look at some rare Linux samples used by Turla that Kaspersky Lab had discovered in 2014. Named PenquinTurla, these samples are also based on LOKI2. Further, the re-analysis showed that all of them use code created between 1999 and 2004.

Remarkably, this code is still being used in attacks. It was spotted in the wild in 2011 when it was found in an attack on defense contractor Ruag in Switzerland that has been attributed to Turla. Then, in March 2017, Kaspersky Lab researchers discovered a new sample of the PenquinTurla backdoor submitted from a system in Germany.It is possible that Turla uses the old code for attacks on highly secure entities that might be harder to breach using its more standard Windows toolset.

"In the late 1990s, no-one foresaw the reach and persistence of a coordinated cyberespionage campaign. We need to ask ourselves why it is that attackers are still able to successfully leverage ancient code in modern attacks. The analysis of the Moonlight Maze samples is not just a fascinating archaeological study; it is also a reminder that well-resourced adversaries aren't going anywhere, it's up to us to defend systems with skills to match," said Juan Andres Guerrero-Saade, Senior Security Researcher, Global Research and Analysis Team Kaspersky Lab.


Mapping Moonlight Maze – reconstructing one of the world's first major threat actors
Victim
Main proxy node e.g. a US library
HRTest relay server
GREAT
KASPERSKY

The newly unearthed Moonlight Maze files reveal many fascinating details about how the attacks were conducted using a complex network of proxies, and the high level of skills and tools used by the attackers. Kaspersky Lab products successfully detect and block malware used by MoonlightMaze and PenquinTurla.

# Pakistan hotline offers safe space for women harassed online

## Cyber bill enforcement remains in question

**LAHORE:** When Pakistani social media starlet Qandeel Baloch was found strangled, a crime to which her brother proudly confessed, thousands of women posted messages denouncing her murder-only to face abuse and threats themselves. Nighat Dad, a human rights activist who founded Digital Rights Foundation, which advocates for free speech and against harassment, said her phone, began ringing off the hook with women seeking advice, fearing they could be targeted next.

She had offered counseling and legal guidance to such victims since setting up her organization in 2012. But the volume of requests shot up after Qandeel's murder last summer. In an effort to deal with this fresh wave, Dad decided to create a hotline in December that began operating from her office in Lahore and now handles up to dozens of calls a day. The result-a safe space for Pakistani women in this deeply patriarchal and religiously conservative country, where online threats sometimes translate into offline violence.

No case epitomizes this phenomenon better than that of Baloch, a polarizing figure who had gained an online following of millions for her daring selfies and provocative videos, including one attacking politicians for discouraging Valentine's day. It was too much to handle for her brother Waseem, currently on trial for her murder, who cited her "intolerable behavior" as the reason behind his crime-one of around a thousand so-called honor killings that take place in Pakistan every year.

### They kill you for everything

The risk is especially high for women from conservative backgrounds, who can at times be blackmailed for even having an account on Facebook or using their real picture. Another common problem is the issue of sexual blackmail-including when a boyfriend seeks nude or semi-nude photos from his girlfriend and later uses the material to manipulate her, threatening to release the images if she does not comply with his demands.

Eman Suleman, a 25-year-old undergraduate student at Lahore's Beacon house National University, found herself at the receiving end of a concerted hate campaign when she and her fellow students put together an exhibition featuring bloodied menstrual pads to spark a conversation about periods. Instead of the passionate debate they had hoped for, they received threats.

**LAHORE: In this photograph, Pakistani lawyer and founder of the Digital Rights Foundation Nighat Dad speaks during an interview with AFP in Lahore. —AFP**

"These anti-secular pages started putting up pictures of us with our personal information then people started messaging us with threats like burn them," she said. "We were really disturbed because of the reaction and because of the messages we were getting and we didn't know what to do." Their parents asked them to stop going to school out of fear they could be attacked. Suleman then got in touch with activist Dad, who was able to draw on past experiences to offer a non-judgmental perspective and provide her with emotional support as she rode out the torrent of abuse. —AFP

# Google adds fact check to global search results

**WASHINGTON:** Google is adding a fact-checking tag to search results globally, its latest initiative to help curb the spread of misinformation and "fake news," the company said yesterday. The new tags, to be used in all languages for users worldwide, will use third-party fact-checkers to indicate whether news items are true, false or somewhere in-between. "For the first time, when you conduct a search on Google that returns an authoritative result containing fact checks for one or more public claims, you will see that information clearly on the search results page," Google said in a blog post.

"The snippet will display information on the claim, who made the claim, and the fact check of that particular claim." The information won't be available for every search result, and there may be conflicting conclusions in some cases, Google said in the blog post, from researcher Cong Yu and Justin Kosslyn of Google's sister company Jigsaw. "These fact checks are not Google's and are presented so people can make more informed judgments," it said.

"Even though differing conclusions may be presented, we think it's still helpful for people to understand the degree of consensus around a particular claim and have clear information on which sources agree." Google has worked with 115 fact-checking groups worldwide for the initiative, which began last year. The move came a day after Facebook added a new tool in news feeds to help users determine whether shared stories are real or bogus.

Fake news became a serious issue in last year's US election campaign, when clearly fraudulent stories circulated on social media, potentially swaying some voters. Concerns have been raised since then about hoaxes and misinformation affecting elections in Europe this year, with investigations showing how "click farms" generate revenue from online advertising using made-up news stories. The moves by both firms aim to change the way news is ranked, diminishing the importance of how often a particular story is shared or clicked on. —AFP