Cybercrime is more of a threat than nation-state hackers

readme.security/cybercrime-is-more-of-a-threat-than-nation-state-hackers-6f6cccf47721

Cynthia Brumfield

By Cynthia Brumfield

Back-to-back security conferences detailed the latest threats posed by malicious nation-states on the one hand and cybercriminals on the other. One takeaway is that cybercrime volumes are more massive and more persistent than the higher profile advanced persistent threats.

On the heels of this year's Cyberwarcon conference, which tackled topics related to advanced persistent threat (APT) actors, the organizers branched off into a new, second-day event called "Brunchcon" that examined the other big basket of cyber threats organizations face: cybercrime.

"I could never pick crimeware over APT or APT over crimeware," Proofpoint vice president of threat research and detection Sherrod DeGrippo said during the first presentation at Brunchcon. "It's like trying to pick your favorite child," she said, even as she acknowledged that Proofpoint built its reputation by working on crimeware.

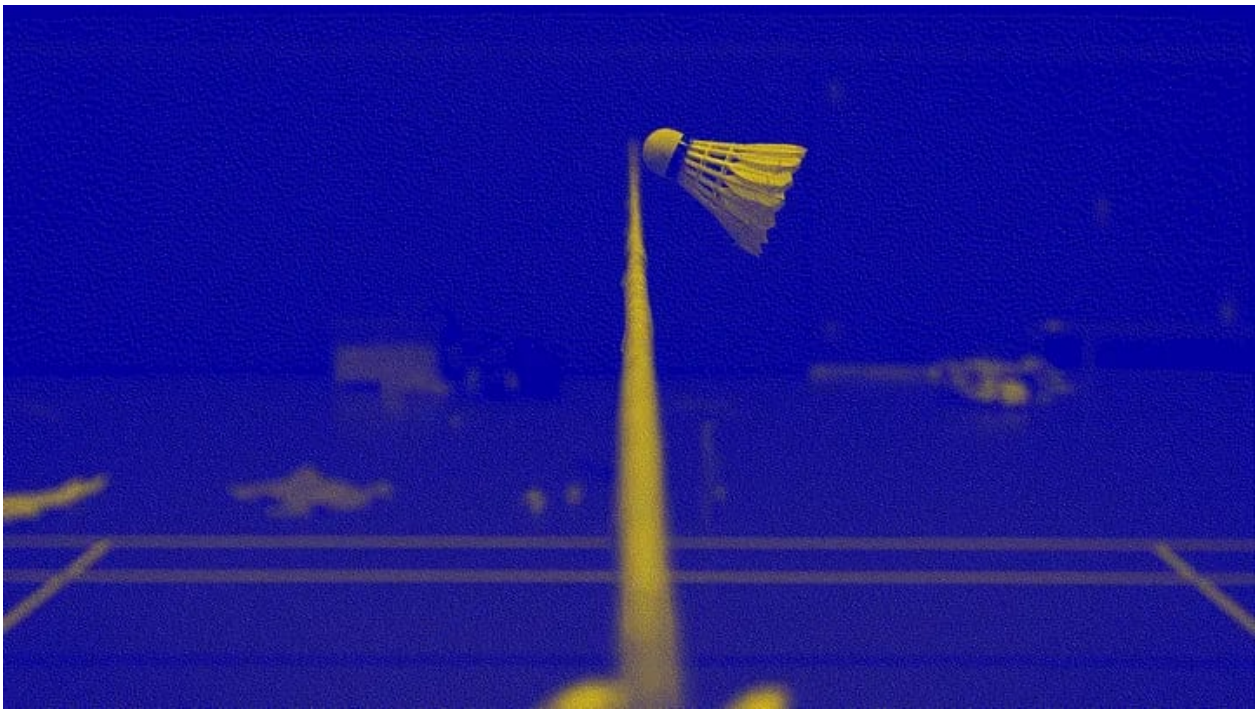
But, "crimeware is more advanced, it's more persistent, it's more a threat. It's more fun. It's cooler. It has weirder stuff. We saw tons of Queen Elizabeth's death lures. And APT guys aren't doing that."

Cybercrime impacts every organization

Although not as headline-grabbing as nation-state attacks, the bread-and-butter threats most cyber defenders face come from criminals, not the Kremlin. “The volumes are massive,” DeGrippo said, a point underscored by other Brunchcon speakers. Red Canary director of intelligence Katie Nickels and Brunchcon emcee told README “I think researchers across the field agree that the predominant threats that we observe affecting organizations every day are cyber-criminal threats.”

“I think the community tends to focus on so-called advanced persistent threats, those state-sponsored actors, because they’re intriguing, they’re interesting, they tend to make headlines,” Nickels said. “But the reality is that the cybercrime actors compromising schools and hospitals with info stealers that can lead to data extortion or ransomware impact every organization.”

Allan Liska, an intelligence analyst at Recorded Future, agreed with DeGrippo and Nickels. “Sherrod had it right,” he told README. “The nation-state actors, for the most part, work nine to five, and then they go home. I know we used to follow some Chinese threat actors who would leave for lunch for an hour every day. They had a badminton porch in their office park. So, they would all go and [play badminton] and they would share scores with each other and they had an ongoing tournament. And you don’t see that with ransomware actors. They just kind of work themselves to death. So, you do have to worry about that,” he said.



Stephan Rothe / Unsplash

The number of ransom extortion sites jumped in 2022

It's difficult to determine whether the number of ransomware incidents has waxed or waned during 2022, Liska told Brunchcon attendees. "What I think is much more interesting is in 2021, and all of 2021, when we pulled things from extortion sites, we were pulling from 44 different extortion sites throughout the whole year," he said.

However, as of Oct. 31, the number of extortion sites from which Recorded Future pulled data rose to 113. "We've also tracked 223 new ransomware variants," Liska said. "And I want to be very clear, most of this is actually stolen code or rebranded stuff. I'm not saying that 223 people have gone out and made brand new ransomware variants, but these are never-seen, never-reported ransomware variants compared to 183 in all of 2021."

Other ransomware trends flagged by Liska include a drop in healthcare and local government ransomware attacks. Attacks on schools are "downish," he said, but they could still end up exceeding those of last year. Notably, "national government attacks are way, way, way up because there are almost none of those in the previous few years," Liska said.

Costa Rica, for example, was thrown into a national emergency when it was struck by a ransomware attack from the Russia-linked Conti ransomware gang earlier this year. Other Latin American nations, including Chile and the Dominican Republic, have been targeted by ransomware attackers over the past several months.

One conclusion Liska takes away from his data is that "we're starting to see ransomware groups reject the [ransomware as a service] model and either going it alone or, if they're adopting the RaaS model, they've also got a side hustle of 'I also have my own ransomware, so maybe sometimes I deploy LockBit, but sometimes I deploy my own ransomware.'"

Consequently, "what we're seeing is LockBit, and then a whole bunch of really also-rans, and very few are cracking even a hundred victims on their extortion site," Liska said. "None that have gotten over 200 victims. So, we're seeing this kind of either centralization to LockBit or moving away from that entirely."

Info stealers enable a new class of attackers

Some new cybercrime threats are on the rise due to the advent of info stealers, Christopher Glyer, a principal security researcher at Microsoft, told Brunchcon attendees. The rise of info stealers "have really enabled an entirely kind of new class of attacker that now is actually targeting enterprises," Glyer said.

Although many of the info stealer groups Microsoft tracks are broadly labeled as Lapsus$, a loosely formed group of hackers notorious for attacking large companies such as Microsoft itself, Nvidia and Samsung for extortion purposes, "there's an entirely new class of actors that we're tracking in the last year and they have wildly different motivations," Glyer said.

“Some of them are extortion operators, some deploy ransomware, some are looking to monetize by targeting high net worth individuals. Others are looking to monetize via selling SIM swapping as a service.”

Among this new class of actors is a group that Microsoft calls DEV-0537, which overlaps Lapsus$. Two other new groups include DEV-0829 (which overlaps a group called Nwgen Team) and DEV-0875 (which overlaps a group called 0ktapus.) Despite their differences, these new operators share some commonalities, including purchasing credits or tokens from info stealers. Surprisingly, many of these groups come from western countries, according to Glyer. “They have native speakers for targeting organizations from a social engineering perspective.”

BEC is on the rise

Another type of cybercriminal activity that is on the rise is business email compromise (BEC), wherein a cybercriminal socially engineers or tricks victims into handing over money. Despite its prevalence, “we’re barely scratching the surface,” Cofense principal threat advisor Ronnie Tokazowski said at Brunchcon. “The scale we’re operating at now, we are barely touching” the vast number of BEC operators out there.

“We’ve had maybe 2,000 arrests, which is great, but we know at least hundreds of thousands of operators are doing some of this stuff, to put that into perspective,” Tokazowski said. “We are absolutely nowhere near where we need to be” in addressing BEC scams.

Attendance at Brunchcon exceeded the organizers’ expectations, so much so they’re considering hosting it as a stand-alone event as early as next May. But, to avoid a possible trademark dispute, Brunchcon will be called Sleuthcon going forward.