United States {CYBERSECURITY} Magazine
A MULTI PLATFORM PUBLISHING PORTAL

Menu

Understanding the Threat

Cyberstalkers: Tools, Tactics and Threats

Patrick Putman

Everyone knows what a stalker is. And unfortunately, many have experienced one first-hand. But now that we are living in the digital age, it has been taken to a new level. These days, cyberstalkers reside on the internet. Offenders are able to track their victims through the use of computers and mobile devices without even leaving home. Unfortunately, cyberstalking is not just limited to trolls, cyberbullies or script kiddies. Hackers and predators alike use this tactic, and it is getting more 'user friendly'.

Most victims are completely unaware they are being tracked. To make matters worse, cyberstalking can be quite difficult to detect. After all, social media anonymity empowers predatory behavior and we often create a full complex map of our entire lives publicly. Cyberstalking is often used in combination with conventional offline stalking methods. Victims are usually singled out for a specific reason.

How cyberstalkers do it

Cyberstalkers employ multiple tools and methods to track and locate their victim. One of the most common is through the use of social engineering. Cyberstalkers may use spear phishing to break into the victim's account or plant spyware. This would allow them to monitor online activity or collect information on their whereabouts.

Bad acting is when the threat actor creates a fake identity to befriend family, friends or even the victim themselves. It can also involve impersonating someone the victim already knows. Cyberstalkers may resort to actual identity theft in an attempt to embarrass, harass or exploit the victim.

An offender may be a skilled hacker with extensive technical knowledge. Stalkers may resort to using hardware such as GPS tracking devices installed on a vehicle. Likewise, they can hack into a computer's on-board camera and microphone to perform stealth reconnaissance. Cyberstalkers may use malware to infect the victim's mobile device in order to exploit the internal GPS locator. They can even spoof a familiar phone number or even clone the victims' phone itself.

A lot of cyberstalkers engage in the Open Source Intelligence (OSINT) tactic known as Doxing. Doxing is the practice of researching, gathering and publishing information via the internet. For example, some methods for doxing include exploiting public records or databases, search engines and social media. Attackers can utilize open-source software to streamline and automate this process. They can also exploit online searches through the use of query hacks such as Google Dorks. Cyberstalkers often spend weeks or even months collecting information to exploit and harass their victims.

Why they do it

A cyberstalkers motivation may involve multiple factors. For example, the predator could have a fixation or physical attraction to the victim. Additionally, the attacker may employ cyberstalking as an intimidate tactic to force a victim into quid pro quo. Financial greed or extortion is also a common motivation.

Cyberstalkers may be suffering from delusions. However, some attackers seek vengeance for a perceived wrongdoing. The motivation could be to embarrass or defame the victim. It could even be a form of sick entertainment.

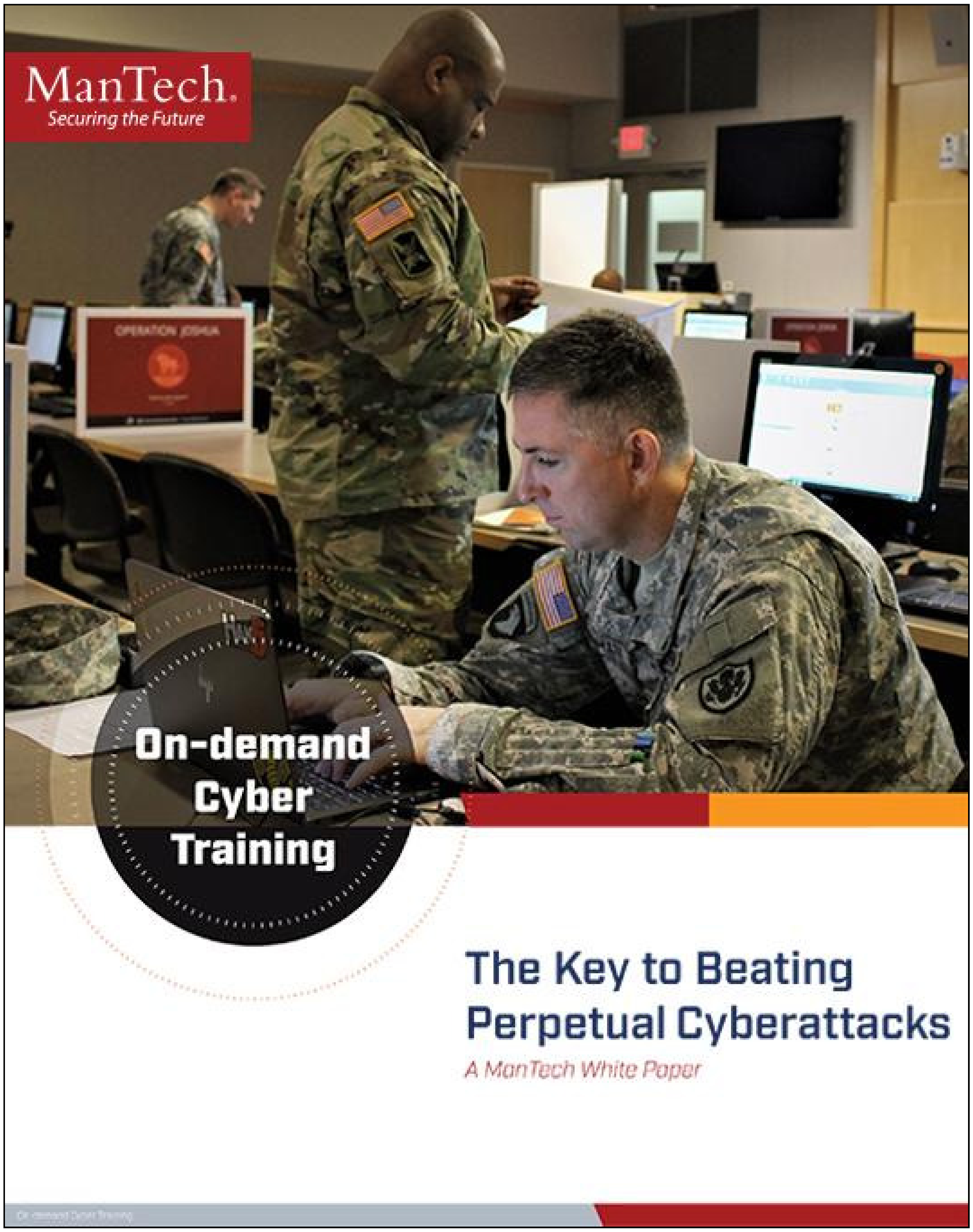
Anyone can become a victim

Cyberstalking is indiscriminate and can happen to people of any gender, sexual orientation or race. The most frightening advantage of cyberstalking is the anonymity. An attacker can learn anything about their target without even leaving the house.

However, there are courses of action you can take. Protect yourself the same way you would against trolling and cyberbullying. Be vigilant and aware of your online presence. Additionally, be aware of your physical surroundings. Show caution with what information you share and who you share it with. If you are a victim, contact your local law enforcement agency immediately. Above all, remember that data breaches are not the only threats that come with cyberstalking. It can result in serious physical harm or even death.

LEAVE A COMMENT

□ I agree to my Facebook data being stored and used as per Privacy Policy



EVENTS CALENDAR

« FEBRUARY 2019 »

SUN	MON	TUE	WED	THU	FRI	SAT
27	28	29	30	31	1	2

« **FEBRUARY 2019** »

3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	1	2

POPULAR ARTICLES

Cyber Threats: Why Cybersecurity Is More Important Than Ever

DevOps Market: Novel Approaches & Products

Put a SOC in it

Starting a Career in Cybersecurity

How to Clean Your Computer and Speed it up

BROWSE BY TOPIC

Engineering and Vulnerability Management

Training and Workforce Development

Industry and Business Best Practices

Data Storage and Access

Legal

RECENT POSTS

Cyber Threats: Why Cybersecurity Is More Important Than Ever

DevOps Market: Novel Approaches & Products

Put a SOC in it

Starting a Career in Cybersecurity

How to Clean Your Computer and Speed it up

Home Magazine Contact Us About Daily Calendar Free Resources Job Board

Advertise With Us Write for Us Privacy Policy Sign Up Log In