Winnti Group, Wicked Panda - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:22:12 UTC

APT group: Winnti Group, Wicked Panda

Names	Winnti Group *(Kaspersky)* Wicked Panda *(CrowdStrike)* Leopard Typhoon *(Microsoft)* G0044 *(MITRE)*
Country	China
Sponsor	State-sponsored
Motivation	Information theft and espionage
First seen	2010
Description	Winnti Group is a threat group with Chinese origins that has been active since at least 2010. The group has heavily targeted the gaming industry, but it has also expanded the scope of its targeting. Some reporting suggests a number of other groups, including APT 41, Axiom, Group 72, APT 17, Deputy Dog, Elderwood, Sneaky Panda, and Ke3chang, Vixen Panda, APT 15, GREF, Playful Dragon, are closely linked to or overlap with Winnti Group. (Trend Micro) The group behind the Winnti malware (which we will call the Winnti group for brevity) sprung up as a band of traditional cyber crooks, comprising black hats whose technical skills were employed to perpetrate financial fraud. Based on the use of domain names they registered, the group started out in the business of fake/rogue anti-virus products in 2007. In 2009, the Winnti group shifted to targeting gaming companies in South Korea using a self-named data- and file-stealing malware. The group, which was primarily motivated by profit, is noted for utilizing self-developed technically-proficient tools for their attacks. They once attacked a game server to illicitly farm in-game currency (“gaming gold”, which also has real-world value) and stole source codes of online game projects. The group also engaged in the theft of digital certificates which they then used to sign their malware to make them stealthier. The Winnti group diversified its targets to include enterprises such as

	those in pharmaceutics and telecommunications. The group has since earned infamy for being involved in malicious activities associated with targeted attacks, such as deploying spear-phishing campaigns and building a backdoor.	
Observed	Sectors: Online video game companies, Aviation, Defense, Education, Financial, Government, Healthcare, Pharmaceutical, Technology, Telecommunications. Countries: Belarus, Brazil, China, Germany, India, Indonesia, Japan, Peru, Philippines, Russia, South Korea, Taiwan, Thailand, USA, Vietnam.	
Tools used	Cobalt Strike, FunnySwitch, Winnti.	
Operations performed	2010	HBGary investigated an information security incident at an American video game company.
	2011	In the autumn of 2011, a Trojan was detected on a huge number of computers – all of them linked by the fact that they were used by players of a popular online game. It emerged that the piece of malware landed on users' computers as part of a regular update from the game's official update server. Some even suspected that the publisher itself was spying on players. However, it later became clear that the malicious program ended up on the users' computers by mistake: the cybercriminals were in fact targeting the companies that develop and release computer games. <https://securelist.com/winnti-more-than-just-a-game/37029/>
	2011	For example, by 2011, one of their victims was Gameforge, a company that offers so-called freemium games: while playing the games is free, it is possible to buy virtual items/money with real money.The Winnti hackers were able to directly access Gameforge's databases and modify accounts to become 'virtually' richer. <https://media.cert.europa.eu/static/MEMO/2019/TLP-WHITE-CERT-EU-MEMO-190725-1.pdf>
	Summer 2014	The Winnti hackers broke into Henkel's network in 2014. We have three files showing that this happened. <https://web.br.de/interaktiv/winnti/english/>
	Aug 2014	This time the operators put such tag in the configuration and it turned out to be the name of the well-known global pharmaceutical company headquartered in Europe. <https://securelist.com/games-are-over/70991/>
	2015	The hackers behind Winnti have also set their sights on Japan's biggest chemical company, Shin-Etsu Chemical. We have in our

	hands several varieties of the 2015 malware which was most likely used for the attack. <https://web.br.de/interaktiv/winnti/english/>
Jul 2015	A BASF spokeswoman tells us in an email that in July 2015, hackers had successfully overcome “the first levels” of defense. <https://web.br.de/interaktiv/winnti/english/>
Oct 2015	Breach of a Vietnamese gaming company <https://blog.vsec.com.vn/apt/initial-winnti-analysis-against-vietnam-game-company.html> During the investigation, a Linux version of Winnti was found. <https://medium.com/chronicle-blog/winnti-more-than-just-windows-and-gates-e4f03436031a>
Feb 2016	Breach of German Steelmaker ThyssenKrupp <https://www.dw.com/en/thyssenkrupp-victim-of-cyber-attack/a-36695341>
Jun 2016	According to Siemens, they were penetrated by the hackers in June 2016. <https://web.br.de/interaktiv/winnti/english/>
Summer 2016	In the case of another Japanese company, Sumitomo Electric, Winnti apparently penetrated their networks during the summer of 2016. <https://web.br.de/interaktiv/winnti/english/>
Mar 2017	Recently, the Winnti group, a threat actor with a past of traditional cybercrime –particularly with financial fraud, has been seen abusing GitHub by turning it into a conduit for the command and control (C&C) communications of their seemingly new backdoor (detected by Trend Micro as BKDR64_WINNTI.ONM). <https://blog.trendmicro.com/trendlabs-security-intelligence/winnti-abuses-github/>
Apr 2018	Breach of German chemicals giant Bayer <https://www.dw.com/en/bayer-points-finger-at-wicked-panda-in-cyberattack/a-48196004>
Nov 2018	Breach of Swiss drug maker Roche <https://www.reuters.com/article/us-germany-cyber/basf-siemens-henkel-roche-target-of-cyber-attacks-idUSKCN1UJ147>
Early 2019	Covestro is regarded as Germany’s most successful spin-off in the recent past. Up until June 2019, they had at least two systems on

		which the Winnti malware had been installed. <https://web.br.de/interaktiv/winnti/english/>
	Early 2019	Another manufacturer of adhesives, Bostik of France, was infected with Winnti in early 2019. <https://web.br.de/interaktiv/winnti/english/>
	2019	Lion Air, Marriott and Valve declined to comment or were not immediately available for comment <https://www.reuters.com/article/us-germany-cyber/basf-siemens-henkel-roche-target-of-cyber-attacks-idUSKCN1UJ147>
	Late 2019	Breach of German chemicals company Lanxess <https://www.tagesschau.de/investigativ/ndr/hackerangriff-chemieunternehmen-101.html>
	Feb 2020	Based on previous knowledge and targeting of the Winnti Group, we assess that this sample was likely used to target Gravity Co., Ltd., a South Korean video game company. The company is known for its Massive Multiplayer Online Role Playing Game (MMORPG) Ragnarok Online, which is also offered as a mobile application. <https://quointelligence.eu/2020/04/winnti-group-insights-from-the-past/>
	Mar 2021	Exchange servers under siege from at least 10 APT groups <https://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/>
Information	<https://blog.trendmicro.com/trendlabs-security-intelligence/pigs-malware-examining-possible-member-winnti-group/> <https://securelist.com/winnti-more-than-just-a-game/37029/> <https://401trg.com/burning-umbrella/> <https://www.blackberry.com/us/en/pdfviewer?file=/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-bb-decade-of-the-rats.pdf>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G0044/>	

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format