APT12, IXESHE, DynCalc, Numbered Panda, DNSCALC, Group G0005

Archived: 2026-04-05 18:21:31 UTC

Domain	ID		Name	Use
Enterprise	T1568	.003	Dynamic Resolution: DNS Calculation	APT12 has used multiple variants of DNS Calculation including multiplying the first two octets of an IP address and adding the third octet to that value in order to get a resulting command and control port.[1]
Enterprise	T1203		Exploitation for Client Execution	APT12 has exploited multiple vulnerabilities for execution, including Microsoft Office vulnerabilities (CVE-2009-3129, CVE-2012-0158) and vulnerabilities in Adobe Reader and Flash (CVE-2009-4324, CVE-2009-0927, CVE-2011-0609, CVE-2011-0611).[2][3]
Enterprise	T1566	.001	Phishing: Spearphishing Attachment	APT12 has sent emails with malicious Microsoft Office documents and PDFs attached.[2][3]
Enterprise	T1204	.002	User Execution: Malicious File	APT12 has attempted to get victims to open malicious Microsoft Word and PDF attachment sent via spearphishing.[2][3]
Enterprise	T1102	.002	Web Service: Bidirectional Communication	APT12 has used blogs and WordPress for C2 infrastructure.[1]