Top malwarové rodiny v České republice – listopad 2024			
Malwarová rodina	**Popis**	**Dopad v ČR**	**Dopad ve světě**
Androxgh0st	Androxgh0st je botnet zaměřený na platformy Windows, Mac a Linux. Pro infikování zařízení využívá několik zranitelností a zaměřuje se hlavně na PHPUnit, Laravel Framework a Apache Web Server. Krade citlivé informace, jako jsou informace o účtu Twilio, SMTP přihlašovací údaje, AWS klíče a podobně. Ke sbírání požadovaných informací používá soubory Laravel. Navíc má různé varianty zaměřené na vyhledávání a krádež různých informací.	7,25 %	5,18 %
BMANAGER	BMANAGER je modulární trojan, který pravděpodobně vytvořil hacker nazvaný Boolka. Boolka nejdříve využíval jen jednoduché skriptovací útoky, ale postupně začal používat sofistikované systémy pro šíření malwaru, včetně trojanu BMANAGER. Tento malware je součástí širší sady, která obsahuje různé komponenty určené ke krádeži dat a přihlašovacích údajů. BMANAGER se šíří především prostřednictvím SQL injection útoků na webové stránky, přičemž využívá zranitelnosti k zachycení uživatelských aktivit a ke krádeži dat.	5,53 %	0,80 %
FormBook	FormBook je škodlivý kód, který krade informace a zaměřuje se na operační systém Windows. Poprvé byl detekován v roce 2016 a je prodáván na nelegálních hackerských fórech. I když je jeho cena relativně nízká, má velmi dobré maskovací schopnosti. FormBook shromažďuje přihlašovací údaje z různých webových prohlížečů, vytváří snímky obrazovky, monitoruje a zaznamenává stisknuté klávesy a může stahovat a spouštět soubory na základě pokynů z C&C serveru.	4,58 %	2,98 %
Remcos	Remcos je RAT (Remote Access Trojan) poprvé detekovaný v roce 2016. Šíří se sám prostřednictvím škodlivých dokumentů Microsoft Office, které jsou připojeny k e-mailovému spamu. Kromě toho dokáže obejít UAC zabezpečení systému Microsoft Windows a spouštět malware s pokročilými právy.	2,67 %	2,41 %
CrimsonRAT	CrimsonRAT (nástroj pro vzdálený přístup) používá programovací jazyk Java a ukrývá se v legitimních souborech. Šíří se prostřednictvím spamových kampaní, které obsahují škodlivé dokumenty Microsoft Office. Útočníkům umožňuje ovládat infikované počítače a provádět škodlivé aktivity.	2,48 %	0,45 %
Torpig	Trojan, který krade informace a sbírá citlivá data a bankovní přihlašovací údaje z infikovaného systému a odesílá je na vzdálený server. Počítače infikované Torpigem také vytvářejí masivní botnet.	2,29 %	0,62 %
TechJourney	TechnoJourney je adware, který se zaměřuje na systémy Mac. Je součástí adwarové rodiny AdLoad a zobrazuje vtíravé reklamy, které mohou vést na škodlivé webové stránky nebo spouštět stahování nechtěných souborů. Může také sledovat uživatelská data a aktivity uživatelů na internetu. Obvykle je distribuován prostřednictvím podvodných webových stránek nebo je připojen k jinému softwaru.	2,29 %	0,16 %

FakeUpdates	FakeUpdates (nebo také SocGholish) je downloader napsaný v jazyce JavaScript. FakeUpdates šíří další malware, včetně GootLoader, Dridex, NetSupport, DoppelPaymer a AZORult.	1,72 %	5,12 %
AgentTesla	AgentTesla je pokročilý RAT, který krade hesla a funguje jako keylogger. Známý je od roku 2014. AgentTesla může monitorovat a zaznamenávat stisknuté klávesy na počítači oběti, systémovou schránku, pořizovat snímky obrazovky nebo krást přihlašovací údaje od různých programů (včetně Google Chrome, Mozilla Firefox a e-mailového klienta Microsoft Outlook). AgentTesla se prodává jako legitimní RAT a zákazníci platí 15–69 dolarů za uživatelskou licenci.	1,53 %	3,10 %
Makoob	Makoob je trojan, který umožňuje získat kontrolu nad infikovanými systémy a krást data nebo instalovat další škodlivé komponenty.	1,53 %	0,60 %